Arithmetic of Strongly Modular $\mathbb{Q}$-curves and the Density of Coprime m-tuples of Algebraic Integers

Dissertation
zur

Erlangung der naturwissenschaftlichen Doktorwürde

(Dr. sc. nat.)

vorgelegt der

Mathematisch-naturwissenschaftlichen Fakultät

der

Universität Zürich

von

Andrea Ferraguti

aus

Italien

Promotionskomitee

Prof. Dr. Joseph Ayoub, Vorsitz

Dr. Peter Bruin

Prof. Dr. Andrew Kresch

Zürich, 2016

Abstract

The main objects of study of this thesis are $\mathbb{Q}$-curves. The first chapter is devoted to giving an introduction to the theory of modular and strongly modular elliptic curves over $\overline{\mathbb{Q}}$. We will review the fundamental work of Ribet on $\mathbb{Q}$-curves as quotients of abelian varieties of GL_2-type and that of Guitart and Quer which characterize strongly modular elliptic curves.

In the second chapter we address the following problem: given a quadratic $\mathbb{Q}$-curve E completely defined over a quadratic field K, how can one *prove* that $L(E,1)=0$, when this is the case? The answer will be given by exhibiting, under the generalized Manin conjecture, an effective integer Q, depending on E and on the choice of an invariant differential ω_E on E, such that $L(E,1)\cdot Q\cdot\sqrt{|\Delta_K|}/\Omega_E$ is an integer. Here Δ_K is the discriminant of K and Ω_E is a quantity related to the infinite part of the period of E. An important ingredient is an algorithm to compute a newform f of level $\Gamma_1(N)$ such that $L(E,s)=L(f,s)L({}^{\sigma}f,s)$, for ${}^{\sigma}f$ the unique Galois conjugate of f.

The third chapter is dedicated to studying strongly modular twists of $\mathbb{Q}$-curves. In the first part, we find necessary and sufficient conditions for the existence of strongly modular twists of quadratic $\mathbb{Q}$-curves over their minimal field of complete definition. We also show how to characterize completely *primitive* twists, which are elliptic curves not isogenous to the base change of a curve over a smaller field. In the second part, we prove that a $\mathbb{Q}$-curve is geometrically isomorphic to a strongly modular one if and only if it is geometrically isomorphic to a $\mathbb{Q}$-curve whose minimal field of complete definition is abelian over $\mathbb{Q}$.

Finally, in chapter four we study a different problem. A classical theorem, originally due to Mertens and Cesàro (independently), states that the natural density of the set of coprime m-tuples of integers is $1/\zeta(m)$, where $\zeta(s)$ is the Riemann zeta function. Given a number field K with ring of integers $\mathcal{O}$, we introduce a notion of density (depending on the choice of a $\mathbb{Z}$-basis for $\mathcal{O}$) for subsets of $\mathcal{O}$ which generalizes the notion of natural density for subsets of $\mathbb{Z}$. We then show that the density of the set of coprime m-tuples of algebraic integers in $\mathcal{O}$ is $1/\zeta_K(m)$, where $\zeta_K(s)$ is the Dedekind zeta function of K. In particular, the density of this set does not depend on the choice of a $\mathbb{Z}$-basis for $\mathcal{O}$.

Zusammenfassung

Die Hauptobjekte dieser Dissertation sind $\mathbb{Q}$-Kurven. Das erste Kapitel gibt eine Einführung in die Theorie der modularen und streng modularen elliptischen Kurven über $\overline{\mathbb{Q}}$. Darin gehen wir auf das fundamentale Werk Ribets über $\mathbb{Q}$-Kurven als Quotienten abelscher Varietäten des Typs GL_2 ein, und auf dasjenige Guitart und Quers, welches streng modulare elliptische Kurven charakterisiert.

Im zweiten Kapitel beschäftigen wir uns mit dem folgenden Problem: Sei E eine quadratische $\mathbb{Q}$-Kurve, welche über einem quadratischen Feld K vollständig definiert ist. Wie kann man *beweisen*, dass $L(E,1)=0$, falls das der Fall ist? Wir geben eine Antwort auf diese Frage, indem wir, mit Hilfe der verallgemeinerten Manin Vermutung, eine effektive ganze Zahl Q finden, welche von E und der Wahl eines invarianten Differentials ω_E auf E abhängt, so dass $L(E,1)\cdot Q\cdot\sqrt{|\Delta_K|}/\Omega_E$ eine ganze Zahl ist. Hierbei ist Δ_K die Diskriminante von K und Ω_E eine Grösse, die mit dem unendlichen Teil der Periode von E zusammenhängt. Ein wichtiger Bestandteil in diesem Prozess ist ein Algorithmus, um eine Neuformen f zum Level $\Gamma_1(N)$ zu berechnen, so dass $L(E,s)=L(f,s)L({}^{\sigma}f,s)$, wobei ${}^{\sigma}f$ das eindeutige Galois-Konjugierte von f ist.

Das dritte Kapitel ist dem Studium streng modularer Twists von $\mathbb{Q}$-Kurven gewidmet. Im ersten Teil finden wir nötige und hinreichende Bedingungen für die Existenz von streng modularen Twist quadratischer $\mathbb{Q}$-Kurven über dem Minimalkörper vollständiger Definition. Desweiteren zeigen wir, wie man primitive Twists charakterisiert, also elliptische Kurven, die nicht isogen zum Basiswechsel einer Kurve über einem kleineren Körper sind. Im zweiten Teil beweisen wir, dass eine $\mathbb{Q}$-Kurve genau dann geometrisch isomorph zu einer modularen Kurve ist, wenn sie geometrisch isomorph zu einer $\mathbb{Q}$-Kurve ist, dessen Minimalkörper vollständiger Definition abelsch über $\mathbb{Q}$ ist.

In Kapitel vier untersuchen wir schliesslich ein anderes Problem. Ein klassisches Theorem, welches auf Mertens und Cesàro (unabhängig voneinander) zurückgeht, besagt, dass die natürliche Dichte der Menge der teilerfremden m-Tupel ganzer Zahlen $1/\zeta(m)$ ist, wobei $1/\zeta(s)$ die Riemannsche Zeta-Funktion ist. Für einen Zahlenkörper K mit Einheitenring $\mathcal{O}$ führen wir den Begriff einer (von der Wahl einer $\mathbb{Z}$-Basis von $\mathcal{O}$ abhängigen) Dichte von Teilmengen von $\mathcal{O}$ ein, welcher den Begriff der natürlichen Dichte von Teilmengen von $\mathbb{Z}$ verallgemeinert. Wir zeigen dann, dass die Dichte der Menge der teilerfremden m-Tupel algebraischer Zahlen in $\mathcal{O}$ $1/\zeta_K(m)$ ist, wobei $\zeta_K(s)$ die Dedekindsche Zeta-Funktion von K ist. Insbesondere hängt die Dichte dieser Menge nicht von der Wahl einer $\mathbb{Z}$-Basis von $\mathcal{O}$ ab.

Acknowledgments

None of the work in this thesis would have been possible without the precious guidance and support of Peter Bruin. Not only he taught me, with an endless patience, a lot about the marvelous world of elliptic curves and modular forms, but he has also been an example to me, of how it is possible to face everyday research and life always with calm and joy. To him it goes my biggest thanks. Of course I am deeply grateful to Prof. Joseph Ayoub and Prof. Andrew Kresch, for giving me the great opportunity of doing my PhD in Zurich.

These years in Zurich would not have been the same without the invaluable presence of Giacomo Micheli. He has been to me a fantastic officemate, a loyal friend, a precious co-worker and, above all, he always believed in me more than what I do. I simply cannot find enough words to thank him.

I met many people at the Institute of Mathematics who enhanced the quality of my life. I wish to thank Prof. Camillo De Lellis and all the members of his research group whom I had the pleasure to meet: Jusuf, Salvatore, Annalisa, Davide, Dominik, Francesco, Guido, Maria, Andrea, for sharing with me numerous and valuable lunch-time discussions. A special thanks goes to Luca, he has been a special friend to me, and to Antonio, for many table tennis games. For a similar reason I would like to thank Michele and Prof. Ashkan Nikeghbali, for helping me re-discovering one of my greatest passions, tennis. I firmly believe that debating our own ideas and learning from other people's ones is of the utmost importance in order to grow up as a person. Thus I want to thank all people that gave me the opportunity of doing that, be that just once or many times: Utsav, Martin, Davide, Patrick, Riccardo, Martina, Tommaso, Alessandra, Alberto, Alberto, Alessandro, Giuseppe. In particular, I would like to thank Prof. Joachim Rosenthal, for many useful suggestions, both in Mathematics and in life.

As anybody who lived in Zurich knows, finding a house here is a hard task. I had the luck of finding immediately two great flatmates: Lilly and Steve. They certainly deserve a huge thanks for making my first times far from home so comfortable.

Living in a new city set me apart from my old friends, but every time I went back to Milan, they have been happy of embracing me. This is one of the main reasons I could find my own equilibrium, and I cannot avoid to warmly thank all of them: Tommy, Fede, Guglielmo, Mono, Ico, Giobbe, Guido, Guido, Paola, Filo, Sarah, Giulia, Espo and all the ones that I surely forgot at the moment of writing.

Knowing that any time I would go back to my old home I would find two persons ready to welcome me with a smile has been a big source of strength for me. For this reason I am enormously grateful to my parents, for their totally unconditional and constant support, and to my brother, Davide, his wife, Valentina and their sons, Riccardo and Giorgio, for their advices and support, and simply for the joy that they give me every time I see them. I cannot tell how proud I am to have such a beautiful family, and if I will ever achieve my life goals, a large part of the merit will be theirs.

Last, but very far from least, a huge thanks goes to Marta. There has not been a single day in the past three and a half years in which she has not been beside me, supporting and accepting me as I am despite my many faults. The possibility of sharing my good and bad moments with her is one of the things that make me enjoy life so much. Thanks.

Contents

Introduction

One of the central problems in number theory is undoubtedly the study of the group of rational points of an elliptic curve over a number field. A theorem of Mordell and Weil (see for example [71]) states that if E is an elliptic curve over a number field K, then the group $E(K)$ of its rational points is a finitely generated abelian group. Thus one can write $E(K) \simeq T \oplus \mathbb{Z}^r$, where T is the torsion subgroup and r is a non-negative integer, called the *algebraic rank* of E. When $K = \mathbb{Q}$, Mazur [49] classified all the (finitely many) finite abelian groups that appear as the torsion subgroup of $E(\mathbb{Q})$. Merel [50] proved that given a positive integer d, there exists a constant c, depending only on d, such that for every elliptic curve E over a number field of degree at most d, the torsion subgroup of E has cardinality at most c. On the other side, the algebraic rank is a much more mysterious invariant, even when $K = \mathbb{Q}$. For example, there is a "folklore" conjecture stating that there are elliptic curves over $\mathbb{Q}$ of arbitrarily high rank. However, up to now, the curve with the largest rank was found by Elkies, and it has (at least) 28 independent points. When all elliptic curves over $\mathbb{Q}$ are ordered in some suitable sense, it is conjectured that elliptic curves with algebraic rank bigger than 1 constitute a subset of density zero. It is also expected that the average rank is $1/2$, but there are heuristics that seem to tend to contradict this (see [4]).

Even at a more basic level, there are no generic algorithms that, given an elliptic curve, can compute its algebraic rank. By a naive point of view, the first thing one might try to do in order to compute the rational points of E, is to write down a Weierstrass equation with coefficients in the ring of integers $\mathcal{O}_K$, and then reduce it modulo (almost) every prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$. This way one gets an elliptic curve $E_\mathfrak{p}$ over a finite field, whose number of rational points $N(\mathfrak{p})$ is easily computable. Heuristically, one hopes that if $N(\mathfrak{p})$ tends to be large enough for many $\mathfrak{p}$'s, the original elliptic curve has a rational point over K. This is the starting observation that led B. Birch and P. Swinnerton-Dyer to consider the L-function $L(E, s)$ attached to E. This is a holomorphic function defined on the half plane $\{s \in \mathbb{C} \colon \Re(s) > 3/2\}$, and it is built by putting together in a suitable way all the $N(\mathfrak{p})$'s (for the precise definition, see section 2.4). For a certain class of elliptic curves, and conjecturally for every elliptic curve, $L(E, s)$ has an analytic continuation to $\mathbb{C}$. The celebrated Birch and Swinnerton-Dyer conjecture (BSD for short) asserts in its weak form that the order of vanishing of $L(E, s)$ in $s = 1$, which is a non-negative integer called the *analytic rank*, coincides with the algebraic rank. Later on, a strong form of the conjecture was proposed, giving a conjectural formula for the first non-vanishing coefficient of the Taylor series of $L(E, s)$ in $s = 1$ (cf. section

2.8). A proof of the BSD conjecture would be a major breakthrough in the theory of rational points of elliptic curves (see for example [45]). Up to now, the weak form of the conjecture is known to be true for elliptic curves over $\mathbb{Q}$ when the analytic rank is at most 1 (see [34], [41] and [55] or the survey in [32]) and a partial generalization of this to $\mathbb{Q}$-curves is the content of [17]. Recent results of C. Skinner [74] prove a partial converse to the Gross-Zagier-Kolyvagin theorem. Apart from these results, very little is known in the higher rank case; moreover it is in general extremely difficult even to verify the BSD conjecture for a given E, in particular for curves of high rank.

When E is an elliptic curve over $\mathbb{Q}$ of conductor N, the modularity theorem (see [79], [80] and [8] or the survey in [20]) asserts that there exists a non-trivial map of algebraic curves $X_0(N) \to E$, called a *modular parametrization*, where $X_0(N)$ is the compact modular curve for the congruence subgroup $\Gamma_0(N)$. An equivalent formulation is that the L-function of E coincides with the L-function $L(f_E, s)$ of a newform f_E of weight 2 and level $\Gamma_0(N)$. This is of crucial importance, since L-functions of newforms are much better understood, and are known to possess an analytic continuation to the whole complex plane. Thus, the study of $L(f_E, s)$ can yield information about the algebraic rank of E.

More generally, we say that an elliptic curve over $\overline{\mathbb{Q}}$ is *modular* if it admits a non-trivial map $X_1(N)_{\overline{\mathbb{Q}}} \to E$ for some $N \in \mathbb{N}$, where $X_1(N)$ is the compact modular curve for the congruence subgroup $\Gamma_1(N)$. In the first chapter of this thesis, we will briefly review the theorems, due to Shimura [69], Ribet [62] and Khare and Wintenberger [39], which show that modular elliptic curves are precisely $\mathbb{Q}$-*curves*, i.e. elliptic curves that are isogenous to all of their Galois conjugates over $\overline{\mathbb{Q}}$. In contrast to the case of elliptic curves over $\mathbb{Q}$, in general the L-function of a modular elliptic curve over $\overline{\mathbb{Q}}$ does not coincide with a product of L-functions of newforms. The $\mathbb{Q}$-curves without complex multiplication (CM for short) which enjoy this property are called *strongly modular*. We will review results of [35] that characterize the class of strongly modular elliptic curves over Galois number fields.

From now on, we assume that all our $\mathbb{Q}$-curves are without CM, therefore we will avoid repeating it every time.

Suppose now that K is a quadratic number field of discriminant Δ_K and that E is a $\mathbb{Q}$-curve completely defined over K (i.e. E and any isogeny to its conjugate are defined over K). This is a sufficient condition to ensure that E is strongly modular. In chapter 2 we address the following problem: how can we decide whether $L(E, 1)$ vanishes or not? Computations with modular symbols can in principle answer the question, but they are inefficient when the conductor of E is large. Alternatively, one can compute $L(E, 1)$ to any given precision; however, it is not a priori clear how to decide whether $L(E, 1)$ is exactly 0 or a very small non-zero number. The same type of problem arises when $L(E, 1) \neq 0$: let $P(E/K)$ be the period of E (cf. subsection 2.8.1). This coincides with the product of the Tamagawa numbers of E with $2^s \cdot \Omega_E / \sqrt{|\Delta_K|}$. Here $s = 0$ if K is complex and $s \in \{0, 1, 2\}$ if K is real (depending on the 2-torsion of E), while Ω_E is the factor which encodes the real periods of E when K is real and the covolume of the period lattice when K is imaginary (cf. section 2.8 for the precise definition); this can be computed efficiently (see for example [16]). Suppose that we can compute the L-ratio $L(E, 1) \cdot \sqrt{|\Delta_K|}/\Omega_E$ to any given precision, finding a value which is very close to a rational number t. How can we *prove* that the L-ratio is exactly t?

Our starting point, in section 2.1, will be elliptic curves over $\mathbb{Q}$. Let $\pi\colon X_0(N) \to E$ be a modular parametrization. If ω_E is a Néron differential on E, then $\pi^*(\omega_E) = c \cdot f$, where $c = c(E, \pi)$ is a non-zero integer (defined up to sign) called the *Manin constant* and $f \in S_2(\Gamma_0(N))$ is a newform. The L-function attached to f coincides with the L-function of E and one can see that $L(f, 1) = -2\pi i \int_0^{i\infty} f(t)dt$ using the formula for the analytic continuation of $L(f, s)$. Now a theorem of Manin and Drinfel'd (see [24] and [46]) shows that $\pi(0) - \pi(i\infty)$ has finite order in $E(\mathbb{Q})$ and this allows us to relate $L(f, 1)$ to the real period Ω_E of E and c. In general it is a very hard problem to compute c, but assuming Manin's conjecture it is possible to find an explicit multiple of c in terms of the $\mathbb{Q}$-isogeny class of E. Eventually, this will permit us to find an effective positive integer $Q = Q(E, \omega_E)$ such that $L(E, 1) \cdot Q/\Omega_E$ is a non-zero integer whenever $L(E, 1) \neq 0$. This gives us a very efficient method to decide whether $L(E, 1) = 0$. In fact this happens if and only if computing $L(E, 1)$ up to a sufficient precision it results that $|L(E, 1)| < \Omega_E/Q$. Moreover, the same result allows us to compute the rational number $L(E, 1)/\Omega_E$ whenever this is different from 0.

After reviewing in sections 1.2 and 2.2 some basic constructions associated to $\mathbb{Q}$-curves proved in [30], [35], [59] and [62], in section 2.3 we will focus our attention on quadratic $\mathbb{Q}$-curves completely defined over a quadratic number field K. Ribet's theorem in [62], together with the results of [39], ensures the existence of a newform $f \in S_2(\Gamma_1(N))$ such that $L(E, s) = L(f, s)L({}^{\sigma}f, s)$, where ${}^{\sigma}f$ is the unique Galois conjugate of f. Section 2.4 is dedicated to explaining how one can compute the Fourier coefficients of f given E and an isogeny from E to its Galois conjugate ${}^{\nu}E$. We implemented this algorithm using Sage [75]; the code can be found in the appendix of the thesis.

The existence of the newform f follows from the fact that the Weil restriction of scalars of E, which is an abelian surface over $\mathbb{Q}$, is $\mathbb{Q}$-isogenous to the abelian variety A_f attached to f by Shimura (see [68]). This is the key fact that will allow us to generalize the "geometric" argument used for elliptic curves over $\mathbb{Q}$ to the case of quadratic $\mathbb{Q}$-curves. Section 2.5 contains the core of our argument. We will show there how to choose an appropriate parametrization starting from the data of E, an invariant differential ω_E and an isogeny $\mu\colon E \to {}^{\nu}E$, and how to apply the Manin-Drinfel'd theorem to this setting in order to again relate $L(E, 1)$ to the period of E and the discriminant of K.

One fundamental difference with the case of elliptic curves over $\mathbb{Q}$ is the fact that there is no direct way to uniquely define a Manin constant. In fact if $\mathcal{E}$ is a Néron model for E over the ring of integers $\mathcal{O}_K$ of K, then $H^0(\mathcal{E}, \Omega^1_{\mathcal{E}/\mathcal{O}_K})$ is a locally free $\mathcal{O}_K$-module of rank 1, but it is not necessarily free. However, the pullback of ω_E under our modular parametrization coincides with $\gamma \cdot h$, for certain $\gamma \in K^*$ and $h \in \langle f, {}^{\sigma}f\rangle_{\mathbb{C}}$. In section 2.6 we will recall, following [30], the definition of the so-called *Manin ideal*, an invariant attached to a modular parametrization $X_1(N) \to E$. Assuming a generalization of Manin's conjecture we will be able to use properties of the Manin ideal to find an explicit rational number whose quotient by $N_{K/\mathbb{Q}}(\gamma)$ is an integer; this, together with a small computation performed in section 2.7, will finally allow us to compute an effective positive integer $Q = Q(E, \omega_E)$ such that $L(E, 1) \cdot \dfrac{\sqrt{|\Delta_K|}}{\Omega_E} \cdot Q$ is an integer.

The main result, stated in section 2.8, can be summarized as follows:

Theorem. Let K be a quadratic number field with discriminant Δ_K and let E be a quadratic $\mathbb{Q}$-curve defined over K. For every finite place v of K, let c_v be the Tamagawa

number of E at v. Let $P(E/K) = \prod_v c_v \cdot 2^s \cdot \frac{\Omega_E}{\sqrt{|\Delta_K|}}$ be the period of E. Suppose that $L(E,1) \neq 0$. Then:

$$L(E,1) \cdot \frac{\sqrt{|\Delta_K|}}{\Omega_E} \in \mathbb{Q}^*.$$

Moreover, assuming the generalized Manin conjecture, if we fix an invariant differential ω_E then there exists an effective positive integer $Q = Q(E, \omega_E)$ such that $L(E,1) \cdot \frac{\sqrt{|\Delta_K|}}{\Omega_E} \cdot Q$ is an integer.

In section 2.9 we will produce, starting from quadratic $\mathbb{Q}$-curves of algebraic rank two, relevant examples of newforms of large level which cannot feasibly be computed using modular symbols. Finally, we will show how to use our result to prove that the analytic rank of these curves is exactly two and how the theorem can be used to compute the L-ratio when the analytic rank of the curve is zero.

The hypothesis that E is K-isogenous to its conjugate, and not only geometrically isogenous, is of the deepest importance in chapter 2, since if it fails E is not strongly modular and therefore its L-function cannot be studied with the same methods. Even if the condition of being a $\mathbb{Q}$-curve is invariant under $\overline{\mathbb{Q}}$-isogeny, the condition of being strongly modular is not; results of [30] and [31] imply in fact that every $\mathbb{Q}$-curve is geometrically isogenous to a strongly modular one. The question we answer in chapter 3 is then the following: which $\mathbb{Q}$-curves are $\overline{\mathbb{Q}}$-*isomorphic* to a strongly modular one? We show that on the contrary to what happens with geometric isogenies, this is quite a restrictive condition. For example, the j-invariant of a $\mathbb{Q}$-curve isomorphic to a strongly modular one has to generate an abelian extension of $\mathbb{Q}$.

As often happens with research, to answer the question above we started from investigating a simple case: the one of quadratic $\mathbb{Q}$-curves, i.e. $\mathbb{Q}$-curves over a quadratic field. In this setting, we can characterize explicitly those curves which admit strongly modular twists in terms of the arithmetic of a certain field over which the curves are completely defined. In the last section of the chapter we prove that this is just a particular instance of a more general result.

The characterization of strongly modular $\mathbb{Q}$-curves over Galois number fields given in [35], which we recall in section 3.2, is formulated using properties of a certain cohomology class $[\xi_K(E)] \in H^2(K/\mathbb{Q}, \mathbb{Q}^*)$ that can be attached to the K-isogeny class of E. In section 3.1, we briefly review some results from the cohomology of profinite groups that we need later.

Let now E be a $\mathbb{Q}$-curve over a Galois number field K. Section 3.3 is dedicated to introduce a fundamental invariant of the K-isogeny class of E, called the *minimal field of complete definition*, which is basically the smallest Galois number field L such that E_L is L-isogenous to all its Galois conjugates. This field plays an important role in the statement of our main theorem of chapter 3.

In studying L-functions of $\mathbb{Q}$-curves, it is useful to distinguish when a $\mathbb{Q}$-curve "comes" up to isogeny from a subfield. We prove in section 3.4 a criterion which allows to decide whether a $\mathbb{Q}$-curve completely defined over an abelian number field L is isogenous to the base-change of a $\mathbb{Q}$-curve completely defined over a Galois subfield K. If this is the case, we say that the curve is *inflated* from K, otherwise we say that it is *primitive*.

The terminology "inflated" is due to the fact that a curve is inflated if and only if its associated cohomology class in $H^2(L/\mathbb{Q}, \mathbb{Q}^*)$ is the image under the inflation map of a cohomology class in $H^2(K/\mathbb{Q}, \mathbb{Q}^*)$.

Section 3.5 is completely dedicated to the study of quadratic $\mathbb{Q}$-curves. Let E be a $\mathbb{Q}$-curve over a quadratic field K which is not K-isogenous to its conjugate. First of all, we show that the minimal field of complete definition L of a quadratic $\mathbb{Q}$-curve is a V_4-extension of $\mathbb{Q}$. The base-changed curve E_L is never strongly modular, but it may have strongly modular quadratic twists. Using a result of [40], we characterize completely those quadratic $\mathbb{Q}$-curves such that E_L has strongly modular quadratic twists. This depends uniquely on the arithmetic of L; more precisely, if $L = \mathbb{Q}(\sqrt{d}, \sqrt{e})$ then the existence of such twists depend on certain quaternion algebras over $\mathbb{Q}$ attached to d and e. Moreover, we are able to determine when there exist primitive strongly modular twists and when there exist inflated ones. As a corollary, we deduce necessary and sufficient conditions for E to have strongly modular twists over K. The existence of primitive and inflated strongly modular twists of E_L are independent: we show this by producing several examples. Finally, If $E_L^{(\lambda)}$ is a primitive strongly modular twist of E_L, we describe some of the properties of the Weil restriction of $E_L^{(\lambda)}$ from L to $\mathbb{Q}$, which is simple and modular.

Let us remark that studying strongly modular twists of quadratic $\mathbb{Q}$-curves might have an interesting application within the problem of computing the rank in families of twists. In fact, a strongly modular quadratic $\mathbb{Q}$-curve necessarily has even rank; it is therefore a natural question to try to understand what the average rank in a family of strongly modular curves is.

Finally, section 3.6 is entirely dedicated to the proof of the following theorem.

Theorem. Let E be a $\mathbb{Q}$-curve over $K = \mathbb{Q}(j(E))$. Then E is $\overline{\mathbb{Q}}$-isomorphic to a strongly modular curve if and only if $K/\mathbb{Q}$ is Galois and the minimal field of definition of E is abelian over $\mathbb{Q}$.

This proves that, in particular, every quadratic $\mathbb{Q}$-curve is isomorphic to a strongly modular one. However, the proof of the theorem is not constructive. In order to prove it, we pass through two main auxiliary results. The first one states that a $\mathbb{Q}$-curve E over a non-Galois number field K cannot be strongly modular. This is proved by showing that the dimension of the endomorphism algebra of the Weil restriction of E from K to $\mathbb{Q}$ is too small. The second auxiliary result, of a more technical nature, states that the 2-torsion in the Brauer group of $\mathbb{Q}$ is generated by certain symmetric cohomology classes living in $H^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\})$. This is useful because it allows to "symmetrize" the cohomology class attached to our $\mathbb{Q}$-curves, making them strongly modular up to twists.

The last chapter is dedicated to a completely different topic. It constitutes a paper, written jointly with Dr. G. Micheli, which is to appear in the Bulletin of the Australian Mathematical Society, and it appears in this thesis in the form in which it will be published.

A very well-known result, which dates back originally to Mertens and Cesàro (independently), asserts that the natural density of the set of coprime m-tuples of integers is $1/\zeta(m)$, where $\zeta(s)$ is the Riemann zeta function. Recall that the natural density of a subset T of $\mathbb{Z}^m$ is defined as the limit, if it exists, of the sequence $a_N := \dfrac{|T \cap [-N, N[^m|}{(2N)^m}$,

and it can be interpreted as the limit of the probability that a uniformly randomly chosen point in the hypercube of side N is in T, as N tends to ∞.

The goal of our paper is to generalize the above result to the ring of integers $\mathcal{O}$ of a number field K. The first problem one encounters is how to generalize the concept of density to subsets of $\mathcal{O}^m$. We chose to use a definition which depends on the choice of a $\mathbb{Z}$-basis of $\mathcal{O}$: if $\psi\colon \mathcal{O}^m \to \mathbb{Z}^{m[K:\mathbb{Q}]}$ is an isomorphism, we define the density of a subset of $\mathcal{O}^m$ as the natural density, if it exists, of its image via ψ.

Now, we say that an element $(\alpha_1, \dots, \alpha_m) \in \mathcal{O}^m$ is a *coprime m-tuple* if the α_i's generate the trivial ideal. Let $S \subseteq \mathcal{O}^m$ be the set of all coprime m-tuples. In section 4.3 we prove the following theorem.

Theorem. The density of S exists and equals $1/\zeta_K(m)$, where ζ_K is the Dedekind zeta function of K. In particular, it does not depend on the choice of a $\mathbb{Z}$-basis for $\mathcal{O}$.

The strategy of the proof is quite simple: for every $t \in \mathbb{N}$ we let $S_t \subseteq \mathcal{O}^m$ be the set of all m-tuples $(\alpha_1, \dots, \alpha_m)$ such that the ideal generated by the α_i's is coprime with the ideals generated by the first t prime numbers. It is not too difficult to compute the density of S_t. It is clear that $S = \bigcap_{t\in\mathbb{N}} S_t$. The technical difficulty is to prove that the density of S exists and coincides with the limit in t of the densities of the S_t's. The key tool is a lemma (cf. [47, Lemma 2]) which allows to compute lattice points inside hypercubes of $\mathbb{R}^d$.

Notation and conventions

For every $N \in \mathbb{N} = \{1, 2, \ldots\}$ we set as usual:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon c \equiv 0 \bmod N \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon c \equiv 0 \bmod N,\ a \equiv d \equiv 1 \bmod N \right\},$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon b \equiv c \equiv 0 \bmod N,\ a \equiv d \equiv 1 \bmod N \right\}.$$

If $G \leq \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup, the space of modular forms of level G and weight $k \in \mathbb{Z}$ is denoted by $M_k(G)$. The subspace of cuspforms will be denoted by $S_k(G)$.

For a Dirichlet character ε modulo N, the space of modular forms (resp. cuspforms) of level $\Gamma_1(N)$, weight k and character ε is denoted by $M_k(\Gamma_1(N), \varepsilon)$ (resp. $S_k(\Gamma_1(N), \varepsilon)$).

The word "newform" means "normalized newform", so if $\sum_{n=1}^{+\infty} a_n q^n$ is the Fourier expansion of a newform then $a_1 = 1$.

The *upper half plane* is the set

$$\mathcal{H} \coloneqq \{z \in \mathbb{C} \colon \Im(z) > 0\}.$$

The *compactified upper half plane* is the set

$$\overline{\mathcal{H}} \coloneqq \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}).$$

This will be given the topology described for example in [20], which makes $\overline{\mathcal{H}}$ a compact topological space. If G is a congruence subgroup and $x, y \in \mathbb{Q}$ are not both zero, the cusp of G corresponding to the equivalence class of $(x \colon y) \in \mathbb{P}^1(\mathbb{Q}) \subseteq \overline{\mathcal{H}}$ under the left action of G on $\mathbb{P}^1(\mathbb{Q})$ will be denoted by $\binom{x}{y}$.

The modular curve for G is denoted by $X(G)$. If $G = \Gamma_0(N)$ (resp. $\Gamma_1(N)$), the modular curve for G is denoted by $X_0(N)$ (resp. $X_1(N)$).

The Jacobian of $X(G)$ will be denoted by $J(G)$. If $G = \Gamma_0(N)$ (resp. $\Gamma_1(N)$), then the Jacobian of $X(G)$ will be denoted by $J_0(N)$ (resp. $J_1(N)$).

For algebraic varieties A, B defined over a field K, when we talk about maps $\varphi\colon A \to B$ we always mean, unless specified otherwise, that φ is also defined over K. If in addition A and B are abelian varieties, $\mathrm{Hom}(A,B)$ is the set of isogenies $A \to B$ defined over K. Therefore when we say that two abelian varieties over K are isogenous we always mean, unless otherwise specified, that they are isogenous over K, and we denote it by $A \sim B$. If F is an extension of K, the set of isogenies defined over F is denoted by $\mathrm{Hom}_F(A,B)$. The dual of an isogeny φ is denoted by $\widehat{\varphi}$. The base-change of A to F is denoted by A_F. The $\mathbb{Q}$-vector space $\mathrm{Hom}_F(A,B) \otimes_{\mathbb{Z}} \mathbb{Q}$ is denoted by $\mathrm{Hom}^0_F(A,B)$. The $\mathbb{Q}$-algebra of the endomorphisms of A is denoted by $\mathrm{End}^0_F(A)$.

For a number field K, the absolute Galois group of K is denoted by G_K. The maximal abelian extension of $\mathbb{Q}$ is denoted by $\mathbb{Q}^{\mathrm{ab}}$ and the Galois group of $\mathbb{Q}^{\mathrm{ab}}$ over $\mathbb{Q}$ is denoted by $G^{\mathrm{ab}}_{\mathbb{Q}}$. All our number fields are contained in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$.

If G is a profinite group acting continuously on a topological abelian group A, we denote by $Z^i(G,A)$ and $B^i(G,A)$ the groups of continuous i-cocycles and i-coboundaries, respectively. The i-th cohomology group is denoted by $H^i(G,A)$. The class of a cocycle $c \in Z^i(G,A)$ in $H^i(G,A)$ is denoted by $[c]$. When G is the Galois group of an extension of fields L/K, we abbreviate $H^i(\mathrm{Gal}(L/K),A)$ into $H^i(L/K,A)$, and the same for cocycles and coboundaries.

Group actions will be denoted in the upper left corner, so if $\sigma \in G$ and $a \in A$ the result of the action of σ on a is ${}^{\sigma}a$. If G is a group and A is a G-module, the submodule of G-invariants is denoted by A^G.

Cyclic groups of order n are denoted by C_n.

Chapter 1

Modular elliptic curves

In this first chapter, we will recollect some of the main results in the theory of (classical) modularity of elliptic curves over $\overline{\mathbb{Q}}$. This is quite a broad topic, embracing different areas of algebraic geometry and number theory. It is not our intention to review all the proof of these results, which often happen to be of a very deep nature. Our goal is to focus on those results which will be used more consistently throughout the rest of this thesis.

After briefly recalling modularity results for elliptic curves over $\mathbb{Q}$ and elliptic curves over $\overline{\mathbb{Q}}$ with CM, we will summarize the proof of Ribet theorem in [62], which describes the class of modular elliptic curves over $\overline{\mathbb{Q}}$ without CM.

In section 1.3, we will recall some of the results of [31] about strongly modular elliptic curves, which are the central objects in chapters 2 and 3.

Let E be an elliptic curve over $\overline{\mathbb{Q}}$.

Definition 1.0.1. We say that E is *modular* if there exists $N \in \mathbb{N}$ and a non-trivial map of algebraic curves $\pi\colon X_1(N)_{\overline{\mathbb{Q}}} \to E$. Such map is called a *modular parametrization*.

Recall that the space of holomorphic differentials $H^0(X_1(N)_{\mathbb{C}}, \Omega^1_{\mathbb{C}})$ can be identified with the space of weight 2 cuspforms for $\Gamma_1(N)$. Thus the pullback via π of a (non-zero) invariant differential ω on E is identified with a weight 2 cuspform, which in some case turns out to be a newform.

Conversely, given a weight 2 newform $f = \sum_{n=1}^{+\infty} a_n q^n$ for a congruence subgroup G, it is possible to construct an abelian variety associated to f. When f has rational Fourier coefficients, this abelian variety is an elliptic curve. In fact, the following fundamental theorem holds.

Theorem 1.0.2 (Shimura, [68])**.** Let $F \coloneqq \mathbb{Q}(a_n\colon n \in \mathbb{N})$ be the number field generated by the Fourier coefficients of f. Then there exists an abelian variety A_f over $\mathbb{Q}$ such that:

i) A_f is a subvariety of $J(G)$;

ii) A_f is simple over $\mathbb{Q}$;

iii) $\dim A_f = [F\colon \mathbb{Q}]$;

iv) $F \simeq \mathrm{End}^0_{\mathbb{Q}}(A_f)$ via the map $a_n \mapsto T_n$, where T_n is the n-th Hecke operator acting on $J(G)$, restricted to A_f.

Let $N \in \mathbb{N}$. For every divisor M of N, choose a set S_M of representatives of the Galois conjugacy classes of newforms in $S_2(\Gamma_1(M))$. Let $S = \bigcup_{M|N} S_M$. The Jacobian of $X_1(N)$ decomposes up to isogeny as

$$J_1(N) \sim_{\mathbb{Q}} \bigoplus_{f \in S} A_f^{m_f} \tag{1.1}$$

where m_f is the number of divisors of N/M_f if f is a newform of level M_f. The analogous statement holds for $\Gamma_0(N)$.

Remark 1.0.3. Note that the following statements are equivalent:

i) there exists a modular parametrization $X_1(N)_{\overline{\mathbb{Q}}} \to E$;

ii) there exists a nonconstant map $J_1(N)_{\overline{\mathbb{Q}}} \to E$;

iii) there exists a newform $f \in S_2(\Gamma_1(N'))$ for some divisor N' of N, and a surjective map $(A_f)_{\overline{\mathbb{Q}}} \to E$.

In fact, i) implies ii) by functoriality, while ii) implies i) for the following reason: if there is a nonconstant map $J_1(N)_{\overline{\mathbb{Q}}} \to E$ then there is also a nonconstant map $J_1(N)_{\mathbb{C}} \to E_{\mathbb{C}}$. Then composing this with the map $X_1(N)_{\mathbb{C}} \to \mathrm{Jac}(X_1(N)_{\mathbb{C}}) \simeq J_1(N)_{\mathbb{C}}$, we get a nonconstant map $X_1(N)_{\mathbb{C}} \to E_{\mathbb{C}}$ (see [20]), and this implies easily the claim.

The fact that iii) implies ii) is clear by (1.1), while ii) implies iii) because the restriction of $J_1(N)_{\overline{\mathbb{Q}}} \to E$ to each $(A_f)_{\overline{\mathbb{Q}}}$ is either constant or surjective.

1.1 Modularity over $\mathbb{Q}$

Let E be an elliptic curve over $\mathbb{Q}$, and let N be its conductor. The following theorem holds:

Theorem 1.1.1 (Modularity theorem)**.** There exists a nonconstant map of algebraic curves $X_0(N) \to E$.

This theorem was proven first in [79] and [80] for semistable curves, and the proof was extended to all elliptic curves in [8]. Note that since there is a natural map $X_1(N) \to X_0(N)$, the modularity theorem implies that every elliptic curve over $\mathbb{Q}$ is modular in the sense of definition 1.0.1.

It is beyond the goal of this thesis to analyze or even summarize the complicated proof of the modularity theorem. However, we will recall some equivalent statements.

Theorem 1.1.2. The following statements are equivalent:

1. there exists a nonconstant map of algebraic curves $X_0(N) \to E$;

2. there exists a nonconstant map $J_0(N) \to E$ of abelian varieties over $\mathbb{Q}$;

3. there exists a newform $f \in S_2(\Gamma_0(N))$ and a nonconstant map $A_f \to E$ of abelian varieties over $\mathbb{Q}$;

4. there exists a newform $f \in S_2(\Gamma_0(N))$ such that $L(E,s) = L(f,s)$;

5. there exists a newform $f \in S_2(\Gamma_0(N))$ with rational Fourier coefficients such that for every prime l, the l-adic Galois representation attached to f by [18] is isomorphic to the Galois representation on the l-adic Tate module of E.

For a proof, see for example [20].

There is a key difference when one wants to generalize this to elliptic curves over $\overline{\mathbb{Q}}$: while properties 1), 2) and 3) directly generalize to modular elliptic curves in the sense of definition 1.0.1, properties 4) and 5) are more subtle. As we will see in section 1.3, the L-function of a modular elliptic curve over a number field in general cannot even be written as a product of L-functions of newforms.

1.2 Modular elliptic curves over $\overline{\mathbb{Q}}$

This section is devoted to review the characterization of the class of modular elliptic curves over $\overline{\mathbb{Q}}$. Let us start by summarizing the situation when E has CM.

1.2.1 Elliptic curves with CM

Let $K \subseteq \mathbb{C}$ be an imaginary quadratic field with ring of integers $\mathcal{O}_K$. Recall that if $\alpha, \beta \in \mathcal{O}_K^*$ and $\mathfrak{m}$ is an integral ideal of K, we write $\alpha \equiv \beta \bmod^\times \mathfrak{m}$ if for every prime ideal $\mathfrak{p}$ dividing exactly $\mathfrak{m}$ with exponent $e_\mathfrak{p} > 0$, one has that $v_\mathfrak{p}(\alpha - \beta) \geq e_\mathfrak{p}$.

Let $\mathfrak{m}$ be an integral ideal of K such that if $\xi \in \mathcal{O}_K^*$ and $\xi \equiv 1 \bmod^\times \mathfrak{m}$, then $\xi = 1$ (note that it is always possible to find such an $\mathfrak{m}$ since $\mathcal{O}_K^*$ is finite). Let $I(\mathfrak{m})$ be the group of fractional ideals of K which are coprime with $\mathfrak{m}$. Then there exists a Hecke character $\chi \colon I(\mathfrak{m}) \to \mathbb{C}^*$ of K such that $\chi((a)) = a$ for all $a \in K$ such that $a \equiv 1 \bmod^\times \mathfrak{m}$. Up to replacing $\mathfrak{m}$ with one of its divisors, we can assume that χ is primitive. Set

$$f_\chi(z) \coloneqq \sum_{\substack{\mathfrak{a} \in I(\mathfrak{m}) \\ \mathfrak{a} \subseteq \mathcal{O}_K}} \chi(\mathfrak{a}) e^{2\pi i N(\mathfrak{a}) z}.$$

Let D be the discriminant of K. Let $N \coloneqq -D \cdot N_{K/\mathbb{Q}}(\mathfrak{m})$ and define the following Dirichlet character on $(\mathbb{Z}/N\mathbb{Z})^*$:

$$\varepsilon(a) = \left(\frac{-D}{a}\right) \cdot \frac{\chi((a))}{a},$$

where $\left(\frac{-D}{\cdot}\right)$ is the usual Kronecker symbol.

Theorem 1.2.1 (Shimura, [69])**.** The following statements hold:

i) f_χ is a newform in $S_2(\Gamma_1(N), \varepsilon)$;

ii) the abelian variety A_{f_χ} is isogenous over $\overline{\mathbb{Q}}$ to a product of copies of an elliptic curve E such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq K$.

Since two elliptic curves E, E' over $\overline{\mathbb{Q}}$ with CM are isogenous if and only if $\mathrm{End}^0_{\overline{\mathbb{Q}}}(E) \simeq \mathrm{End}^0_{\overline{\mathbb{Q}}}(E')$, the above theorem shows that if E is an elliptic curve over $\overline{\mathbb{Q}}$ with CM by an imaginary quadratic field K then there exist a non-trivial map $(A_f)_{\overline{\mathbb{Q}}} \to E$ for some newform $f \in S_2(\Gamma_1(N), \varepsilon)$, and thus E is modular by Remark 1.0.3.

1.2.2 Elliptic curves without CM

Let us now switch to the case of elliptic curves without CM.

Definition 1.2.2. An elliptic curve $E/\overline{\mathbb{Q}}$ is called a $\mathbb{Q}$-*curve* if E is isogenous to ${}^{\sigma}E$ for every $\sigma \in G_{\mathbb{Q}}$.

We say that E is *completely defined* over a Galois number field K if there exists a model E_0 of E over K such that E_0 is K-isogenous to ${}^{\sigma}E_0$ for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Note that by the theory of complex multiplication, every elliptic curve over $\overline{\mathbb{Q}}$ with CM is a $\mathbb{Q}$-curve.

Theorem 1.2.3 (Ribet, [62])**.** An elliptic curve $E/\overline{\mathbb{Q}}$ without CM is modular if and only if it is a $\mathbb{Q}$-curve.

We have to specify that Ribet proved this theorem assuming Serre's conjecture, which was only proved some years later in [39].

We will dedicate the rest of this section to explaining the proof of Theorem 1.2.3, following [62]. Let us start by recalling the following definition.

Definition 1.2.4. Let A be an abelian variety over $\mathbb{Q}$. We say that A is *of* GL_2*-type* if there exists a number field F with $[F\colon \mathbb{Q}] = \dim A$ and an embedding

$$F \hookrightarrow \mathrm{End}^0_{\mathbb{Q}}(A).$$

If A is an abelian variety of GL_2-type and F is a number field of degree $g = \dim A$ acting on A up to isogeny, then the Tate module $V_l(A)$ is a free $\mathbb{Q}_l$-module of rank $2g$, and thus $V_l(A)$ is a free $F \otimes_{\mathbb{Q}} \mathbb{Q}_l$-module of rank 2. Therefore the action of $G_{\mathbb{Q}}$ on $V_l(A)$ yields a Galois representation with values in $\mathrm{GL}_2(F \otimes_{\mathbb{Q}} \mathbb{Q}_l)$, and this is the reason why A is called "of GL_2-type".

Notice that an abelian variety A of GL_2-type is simple if and only if $\mathrm{End}^0_{\mathbb{Q}}(A)$ is a number field of degree $\dim A$.

Remark 1.2.5. If $f \in S_2(\Gamma_1(N))$ is a newform, the abelian variety A_f attached to f described in Theorem 1.0.2 is of GL_2-type.

The strategy of Ribet's proof of Theorem 1.2.3 is to prove the following statements:

1. if an elliptic curve E without CM is a quotient of an abelian variety of GL_2-type, then it is a $\mathbb{Q}$-curve;

2. if E is a $\mathbb{Q}$-curve without CM, then E is a quotient of an abelian variety of GL_2-type;

3. every simple abelian variety of GL_2-type is isogenous to A_f for some newform $f \in S_2(\Gamma_1(N))$.

Note that point 1), together with Remark 1.2.5, proves one of the two directions of Theorem 1.2.3, namely the fact that if E is modular, then it is a $\mathbb{Q}$-curve. The proof of this relies on the following propositions.

Let A be a simple abelian variety of GL_2-type and let $F = \mathrm{End}^0_{\mathbb{Q}}(A)$.

Proposition 1.2.6 (Shimura, [70])**.** Suppose that $A_{\overline{\mathbb{Q}}}$ has a non-zero abelian subvariety of CM-type. Then $A_{\overline{\mathbb{Q}}}$ is isogenous to a power of a CM elliptic curve.

Proposition 1.2.7. Suppose that $A_{\overline{\mathbb{Q}}}$ has no non-zero abelian subvarieties of CM-type. Then $A_{\overline{\mathbb{Q}}} \sim B^n$ for some simple abelian variety B over $\overline{\mathbb{Q}}$ and some $n \in \mathbb{N}$. In particular, if $\dim B = 1$, then B is a $\mathbb{Q}$-curve.

Proof. Let $A_{\overline{\mathbb{Q}}} \sim \prod_i B_i^{n_i}$ be the decomposition of $A_{\overline{\mathbb{Q}}}$ up to isogeny. Since F is a field, it acts on each B_i. Therefore $[F\colon \mathbb{Q}]$ divides $2n_i \dim B_i$ for all i (see for example [54]). On the other hand, $[F\colon \mathbb{Q}] = \dim A = \sum_i n_i \dim B_i$, so that $[F\colon \mathbb{Q}] \geq n_i \dim B_i$. Thus for all i we have that $[F\colon \mathbb{Q}] = n_i \dim B_i$ or $[F\colon \mathbb{Q}] = 2n_i \dim B_i$. However, the second case is impossible by hypothesis. Hence, $[F\colon \mathbb{Q}] = n_i \dim B_i = \sum_i n_i \dim B_i$, which shows that $A_{\overline{\mathbb{Q}}} \sim B^n$ for some simple abelian variety B. Since A is defined over $\mathbb{Q}$, we have that $A = {}^{\sigma}A$ for all $\sigma \in G_{\mathbb{Q}}$, so that $B \sim {}^{\sigma}B$ for all σ by the uniqueness of the decomposition up to isogeny. □

Let us now pass to the proof of point 2). First, we introduce a tool which plays a fundamental role in the proof of the theorem and in the rest of this thesis.

Definition 1.2.8. Let X be a scheme over a scheme T. Let $T \to S$ be a morphism of schemes. The object which represents the functor

$$\mathbf{Sch}/S \to \mathbf{Set}$$

$$C \mapsto X(C_T),$$

if it exists, is called the *Weil restriction* or *restriction of scalars* of X and is denoted by $\mathrm{Res}_{T/S}(X)$.

Notice that the restriction of scalars, seen as a functor $\mathbf{Sch}/S \to \mathbf{Sch}/T$, is the adjoint of the functor "extension of scalars" $\mathbf{Sch}/T \to \mathbf{Sch}/S$ mapping X to X_S. We will only be interested in restriction of scalars of abelian varieties, so let us recall the following result.

Lemma 1.2.9 ([52])**.** Let $K \subseteq L$ be a finite, separable field extension and let A be an abelian variety over L. The restriction of scalars $\mathrm{Res}_{L/K}(A)$ exists, and is an abelian variety. Moreover, there is an isomorphism

$$\mathrm{Res}_{L/K}(A)_{\overline{K}} \simeq \prod_{\sigma\colon K \to \overline{L}} {}^{\sigma}A,$$

so that $\dim \mathrm{Res}_{L/K}(A) = [L\colon K] \cdot \dim A$.

Let $E/\overline{\mathbb{Q}}$ be a $\mathbb{Q}$-curve without CM. It is possible to construct an element of $H^2(G_\mathbb{Q}, \mathbb{Q}^*)$ (where $G_\mathbb{Q}$ acts trivially on $\mathbb{Q}^*$) attached to E in the following way: for every $\sigma \in G_\mathbb{Q}$ choose an isogeny $\mu_\sigma \colon {}^\sigma E \to E$ so that the system $\{\mu_\sigma\}_{\sigma \in G_\mathbb{Q}}$ is locally constant. Then let

$$\xi(E) \colon G_\mathbb{Q} \times G_\mathbb{Q} \to \mathbb{Q}^*$$
$$(\sigma, \tau) \mapsto \mu_\sigma {}^\sigma\mu_\tau \mu_{\sigma\tau}^{-1},$$

where we identify $\mathrm{End}^0_\mathbb{Q}(E)$ with $\mathbb{Q}$. This is a 2-cocycle whose class in $H^2(G_\mathbb{Q}, \mathbb{Q}^*)$ depends only on the isogeny class of E and not on the choice of the μ_σ's. If E is completely defined over a Galois number field K, one can choose K-isogenies μ_σ for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and in the same way obtain a 2-cocycle $\xi_K(E)$ whose class in $H^2(K/\mathbb{Q}, \mathbb{Q}^*)$ depends only on the K-isogeny class of E. Note that the inflation of $[\xi_K(E)] \in H^2(K/\mathbb{Q}, \mathbb{Q}^*)$ to $H^2(G_\mathbb{Q}, \mathbb{Q}^*)$ coincides with $[\xi(E)]$.

Suppose E is defined over a number field K. Up to enlarging K, we can assume that it is Galois and that E is completely defined over K. Let $\xi_K \in Z^2(K/\mathbb{Q}, \mathbb{Q}^*)$ be a cocycle attached to E as above, and let ξ be its inflation to $G_\mathbb{Q}$.

Theorem 1.2.10 (Tate, [66])**.** Let $G_\mathbb{Q}$ act trivially on $\overline{\mathbb{Q}}^*$. Then $H^2(G_\mathbb{Q}, \overline{\mathbb{Q}}^*) = 0$.

By the theorem above, there exists a locally constant map $\alpha \colon G_\mathbb{Q} \to \overline{\mathbb{Q}}^*$ such that $\xi(\sigma, \tau) = \dfrac{\alpha(\sigma)\alpha(\tau)}{\alpha(\sigma\tau)}$. Up to enlarging K, we can identify α with a map defined on $\mathrm{Gal}(K/\mathbb{Q})$. Let F be the number field generated by the values of α.

Now let $B \coloneqq \mathrm{Res}_{K/\mathbb{Q}}(E)$. There is a decomposition

$$B_K \simeq \prod_{\sigma \in G} {}^\sigma E$$

and thus

$$\mathrm{End}^0_\mathbb{Q}(B) \simeq \prod_\sigma \mathrm{Hom}^0_K({}^\sigma E, E).$$

To describe the ring structure of $\mathrm{End}^0_\mathbb{Q}(B)$, note that since E has no CM, $\mathrm{Hom}^0_K({}^\sigma E, E)$ is a 1-dimensional $\mathbb{Q}$-vector space generated by an isogeny $\mu_\sigma \colon {}^\sigma E \to E$. Let

$$\mathcal{R} \coloneqq \mathrm{End}^0_\mathbb{Q}(B) \simeq \prod_{\sigma \in G} \mathbb{Q} \cdot \mu_\sigma$$

and let λ_σ be the element of $\mathcal{R}$ corresponding to μ_σ. The map λ_σ acts on B_K by sending the factor ${}^{\tau\sigma}E$ to ${}^\tau E$ by ${}^\tau\mu_\sigma$. Hence, keeping in mind that $\mu_\sigma {}^\sigma\mu_\tau = \xi_K(\sigma, \tau)\mu_{\sigma\tau}$ for all $\sigma, \tau \in G$, we get that

$$\lambda_\sigma \lambda_\tau = \xi_K(\sigma, \tau)\lambda_{\sigma\tau}.$$

Therefore there exists a surjective homomorphism of $\mathbb{Q}$-algebras

$$\varphi \colon \mathcal{R} \to F$$
$$\lambda_\sigma \mapsto \alpha(\sigma).$$

Since $\mathcal{R}$ is semisimple, the kernel of φ is principal, generated by some central idempotent. Let ω be the complementary idempotent and let $m \in \mathbb{N}$ be such that $m\omega \in \mathrm{End}(B)$; [62, Proposition 6.5] and [62, Corollary 6.6] show that $A \coloneqq m\omega(B)$ is an abelian variety

of GL_2-type whose algebra of endomorphisms is isomorphic to F. Since B_K decomposes up to isogeny as E^n for some n, the same must be true for A_K. This proves that E is a quotient of A_K.

Point 3) can be stated as follows.

Theorem 1.2.11 ([62, Theorem 4.4] and [39, Theorem 10.1])**.** Let A be a simple abelian variety of GL_2-type. Then A is isogenous to a $\mathbb{Q}$-simple factor of $J_1(N)$ for some $N \geq 1$.

The essence of the proof is the following: if $V_l(A)$ is the l-adic Tate module of A, and $F = \mathrm{End}^0(A)$, then for every prime ideal $\lambda \subseteq \mathcal{O}_F$ the F_λ-module $V_l(A) \otimes_{F \otimes \mathbb{Q}_l} F_\lambda$ defines a 2-dimensional λ-adic Galois representation ρ_λ. Let $\overline{\rho_\lambda}$ be the residual representation. Ribet showed that $\overline{\rho_\lambda}$ is odd and absolutely irreducible for almost all λ, and that there exist an infinite set of λ's such that if $\overline{\rho_\lambda}$ is modular, then it comes from a newform f of weight 2 and fixed level. This gives, via Faltings' theorem, an isogeny $A_f \to A$. By Khare and Wintenberger's theorem, all such $\overline{\rho_\lambda}$ are modular, and the proof is complete.

1.3 Strongly modular abelian varieties

There is a fundamental difference between elliptic curves over $\mathbb{Q}$ and $\mathbb{Q}$-curves over bigger number fields: while, as we have seen, if E is an elliptic curve over $\mathbb{Q}$, its L-function coincides with the L function of some newform f, the same is not true in general for $\mathbb{Q}$-curves. This motivates the following definition, given in [35].

Definition 1.3.1. An abelian variety A over a number field K is called *strongly modular* if there exist $N_1, \ldots, N_t \in \mathbb{N}$ and newforms $f_i \in S_2(\Gamma_1(N_i))$ for $i = 1, \ldots, t$ such that

$$L(A/K, s) \sim \prod_{i=1}^{n} L(f_i, s),$$

where $\sim$ denotes equality up to a finite number of Euler factors.

The following three results describe how to read off strong modularity of A from the restriction of scalars from K to $\mathbb{Q}$.

Lemma 1.3.2 ([35, Lemma 2.2])**.** An abelian variety $B/\mathbb{Q}$ is of GL_2-type if and only if all its $\mathbb{Q}$-simple factors up to isogeny are of GL_2-type.

Proposition 1.3.3 ([35, Proposition 2.3])**.** An abelian variety $B/\mathbb{Q}$ is strongly modular over $\mathbb{Q}$ if and only if it is of GL_2-type.

Proposition 1.3.4. An abelian variety A over a number field K is strongly modular if and only if $\mathrm{Res}_{K/\mathbb{Q}}(A)$ is of GL_2-type.

Proof. Let $B \coloneqq \mathrm{Res}_{K/\mathbb{Q}}(A)$. Since $L(A/K, s) = L(B/\mathbb{Q}, s)$ (see [52]), A/K is strongly modular if and only if $B/\mathbb{Q}$ is strongly modular. By Proposition 1.3.3, this holds precisely when B is of GL_2-type. □

Notice that when $B = \mathrm{Res}_{K/\mathbb{Q}}(A)$ is of GL_2-type, then $B \sim \prod_{i=1}^{n} A_{f_i}$ for some newforms $f_1, \ldots, f_n$. Thus, A/K is strongly modular if and only if

$$L(A/K, s) = \prod_{i=1}^{n} L(f_i, s).$$

The next lemma shows that for strongly modular abelian varieties, the factorization of the L-function into L-functions of newforms is unique up to reordering of the factors.

Lemma 1.3.5. Let A/K be a strongly modular abelian variety. Then the newforms $f_1, \ldots, f_n$ such that $L(A/K, s) = \prod_{i=1}^{n} L(f_i, s)$ are unique, up to reordering.

Proof. Let $B = \mathrm{Res}_{K/\mathbb{Q}}(A)$, so that $L(B/\mathbb{Q}, s) = \prod_{i=1}^{n} L(f_i, s)$. Let $\{g_1, \ldots, g_m\}$ be another set of newforms with $L(B/\mathbb{Q}, s) = \prod_{i=1}^{m} L(g_i, s)$. Since $\prod_{i=1}^{n} L(f_i, s) = \prod_{j=1}^{m} L(g_j, s)$, the Dirichlet series of the left hand side and the right hand side coincide (in a suitable right half-plane of convergence). Thus for every prime p,

$$\sum_{i=1}^{n} a_p(f_i) = \sum_{j=1}^{m} a_p(g_j), \tag{1.2}$$

where $a_p(f_i)$ (resp. $a_p(g_j)$) is the p-th coefficient in the q-expansion of f_i (resp. g_j).

For every newform $f \in S_2(\Gamma_1(M), \varepsilon)$ and every prime l not dividing M, we denote by $\rho_l(f)$ the l-adic Galois representations attached to f (see [18]). Recall that this is a 2-dimensional, irreducible representation with values in a finite extension of $\mathbb{Q}_l$ with the property that

$$\mathrm{Tr}(\rho_l(f)(\mathrm{Frob}_p)) = a_p(f), \quad \text{for all primes } p \nmid Ml.$$

Now let N be the product of all primes dividing the levels of the f_i's and g_j's and let l be a prime not dividing N. Equation (1.2) implies that

$$\mathrm{Tr}\left(\bigoplus_{i=1}^{n} \rho_l(f_i)\right)(\mathrm{Frob}_p) = \mathrm{Tr}\left(\bigoplus_{j=1}^{m} \rho_l(g_j)\right)(\mathrm{Frob}_p) \quad \forall\, p.$$

It is well-known that semisimple, finite-dimensional Galois representations in characteristic 0 are completely determined up to isomorphism by their traces at Frob_p for every p in a set of density 1 (see for example [19, Lemma 3.2]. Thus, the representations $\bigoplus_{i=1}^{n} \rho_l(f_i)$ and $\bigoplus_{j=1}^{m} \rho_l(g_j)$ are isomorphic. By looking at the dimension, we have that $n = m$ necessarily. Moreover, since all the components are irreducible, we can assume up to reordering that

$$\rho_l(f_i) \simeq \rho_l(g_i) \quad \forall\, i \in \{1, \ldots, n\}.$$

It follows that for all $i \in \{1, \ldots, n\}$ we have that $a_p(f_i) = a_p(g_i)$ for all primes p. Now [53, Theorem 4.6.19] shows that $f_i = g_i$. This is done first by showing that the levels of f_i and g_i coincide by looking at the functional equation of their L-functions and then using the multiplicity one principle for newforms. □

Chapter 2

L-functions of quadratic $\mathbb{Q}$-curves

In this chapter, we will study the L-function of a $\mathbb{Q}$-curve E completely defined over a quadratic field K. An elliptic curve with this property is strongly modular; we will show how to make use of this property to compute an effective rational multiple of the period of E, when E has analytic rank 0. We start by looking at elliptic curves over $\mathbb{Q}$, focusing on the properties that can be generalized to the case of $\mathbb{Q}$-curves.

2.1 Elliptic curves over $\mathbb{Q}$

Let E be an elliptic curve over $\mathbb{Q}$ with conductor N and let $\pi\colon X_0(N) \to E$ be a modular parametrization. If ω_E is a Néron differential on E, the multiplicity one principle shows that the pullback $\pi^*(\omega_E)$ is a multiple of a newform $f \in S_2(\Gamma_0(N))$ by a constant $c \in \mathbb{Q}^*$, called the *Manin constant*. Note that choosing ω_E is equivalent to choosing the sign of c.

Theorem 2.1.1 (Edixhoven, [25])**.** The Manin constant is an integer.

Let now E' be another elliptic curve over $\mathbb{Q}$ of conductor N, and let $\pi\colon X_0(N) \to E$ and $\pi'\colon X_0(N) \to E'$ be two modular parametrizations. We say that π' *dominates* π if there is exists a $\mathbb{Q}$-isogeny $\psi\colon E' \to E$ such that $\psi \circ \pi' = \pi$. This relation defines a partial ordering on the set of isomorphism classes of pairs (π', E'), where E' is an elliptic curve $\mathbb{Q}$-isogenous to E and $\pi'\colon X_0(N) \to E'$ is a modular parametrization. We write $(\pi', E') \geq (\pi, E)$ if π' dominates π. The map π is called a *strong modular parametrization* if it is a maximal element with respect to this ordering. It is clear that a strong parametrization is unique up to isomorphism; moreover it can be shown that every modular parametrization factors through a strong one. The Manin conjecture for elliptic curves over $\mathbb{Q}$ can be stated as follows:

Conjecture 2.1.2 (Manin conjecture)**.** The Manin constant of a strong parametrization is ± 1.

Results in this direction are presented in [1], [25] and [49]. From now on, let us fix a modular parametrization $\pi\colon X_0(N) \to E$. Let $f(z) = \sum_{n=1}^{+\infty} a_n e^{2\pi i z} \in S_2(\Gamma_0(N))$ be the newform attached to E by the modularity theorem. One of the consequences of the

Modularity theorem is that the L-function of E coincides with the L-function of f. The formula for the analytic continuation of the L-function of f shows us that

$$L(f,s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty f(it) t^s \frac{dt}{t}$$

and therefore

$$L(E,1) = L(f,1) = -2\pi i \int_0^{i\infty} f(z)dz. \tag{2.1}$$

Since $\pi^*(\omega_E) = c \cdot f$ for some $c \in \mathbb{Z}$, one has that

$$c \cdot L(f,1) = \int_{\{0,i\infty\}} \frac{f(q)}{q} dq = \int_{\pi_*(\{0,i\infty\})} \omega_E, \tag{2.2}$$

where $\{0, i\infty\}$ denotes the image in $H_1(X_0(N), \mathbb{R})$ of any path from 0 to $i\infty$ in the compactified upper half plane $\mathcal{H}^*$ and π_* denotes the induced map $H_1(X_0(N), \mathbb{R}) \to H_1(E, \mathbb{R})$. Note that π maps points in $\mathcal{H}^*$ lying on the imaginary axis to real points of E, because complex conjugation on $X_0(N)$ corresponds to reflection with respect to the imaginary axis in $\mathcal{H}^*$, and π commutes with complex conjugation since it is defined over $\mathbb{Q}$. Moreover, the cusps 0 and $i\infty$ of $\Gamma_0(N)$ are defined over $\mathbb{Q}$ and therefore $\pi(0), \pi(i\infty) \in E(\mathbb{Q})$, but not necessarily $\pi(0) = \pi(i\infty)$. However, we have the following result.

Theorem 2.1.3 (Manin–Drinfel'd, [46] and [24])**.** Let G be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and let X_G be the corresponding modular curve. If α, β are two cusps for G, then the class $\{\alpha, \beta\} \in H_1(X_G, \mathbb{R})$ belongs to $H_1(X_G, \mathbb{Q})$.

As an immediate corollary, $\pi(0) - \pi(i\infty)$ is a torsion point in $E(\mathbb{Q})$. If $t = |E(\mathbb{Q})_{\mathrm{tors}}|$ then $t\pi_*(\{0, i\infty\}) \in H_1(E, \mathbb{Z})$ and so $t\pi(0) = t\pi(\infty)$. Since E is defined over $\mathbb{R}$, complex conjugation on $E(\mathbb{C})$ defines a involution $E(\mathbb{C}) \to E(\mathbb{C})$ and consequently an involution $\iota \colon H_1(E(\mathbb{C}), \mathbb{Z}) \to H_1(E(\mathbb{C}), \mathbb{Z})$. Using the uniformization theorem for elliptic curves, it is easy to see (cf. Lemma 2.5.4) that there exists a $\mathbb{Z}$-basis $\{\gamma_1, \gamma_2\}$ of $H_1(E(\mathbb{C}), \mathbb{Z})$ such that $\iota(\gamma_1) = \gamma_1$. The real period of E is defined as $\Omega_E := \int_{\gamma_1} \omega_E$; up to replacing γ_1 by $-\gamma_1$ we can assume that $\Omega_E > 0$. By what we said above, it follows that $t\pi_*(\{0, i\infty\}) = M\gamma_1$ for some $M \in \mathbb{Z}$. Putting everything together, we finally get

$$L(E,1) = \frac{M \cdot \Omega_E}{c \cdot |E(\mathbb{Q})_{\mathrm{tors}}|}. \tag{2.3}$$

Now we would like to deduce from (2.3) an effective integer Q such that $\dfrac{L(E,1)}{\Omega_E} \cdot Q$ is a non-zero integer, under the assumption that $L(E,1) \neq 0$. Since $|E(\mathbb{Q})_{\mathrm{tors}}|$ and Ω_E can easily be computed (see for example [15, Algorithm 7.4.7] or [16]), this would give us an efficient way to decide if $L(E,1)$ vanishes or not, by computing $L(f,1) = L(E,1)$ with a sufficient precision, and to compute $\dfrac{L(E,1)}{\Omega_E}$ whenever $L(E,1) \neq 0$. In order to do this, we need to find an explicit multiple of c. In principle one could assume that E is the strong curve in its isogeny class, so that under conjecture 2.1.2 one can assume that $c = 1$, then compute its period and finally use the absolute bound on $|E(\mathbb{Q})_{\mathrm{tors}}|$ to get

our desired Q. In [29], the author proves that there is an algorithm which allows to do that in polynomial time with respect to the conductor of E. However, our philosophy is to avoid computing with modular symbols, since this can take a huge amount of time when the conductor of E is large. Therefore we will show how to find a multiple of c, which depends only on E, assuming conjecture 2.1.2 and a certain condition on π that we will explain below. For the rest of this section, we will assume that E does not have CM. Let $\pi'\colon X_0(N) \to E'$ be a strong modular parametrization which dominates π. Let $\omega_{E'}$ be a Néron differential on E'. Let $\psi\colon E' \to E$ be the isogeny such that $\psi \circ \pi' = \pi$. Then $\psi^*(\omega_E) = c \cdot \omega_{E'}$ and since the dual isogeny $\widehat{\psi}$ extends to a map of Néron models it is clear that $\widehat{\psi}^*(\omega_{E'}) = a \cdot \omega_E$ for some $a \in \mathbb{Z}$. Since $\psi \circ \widehat{\psi}$ coincides with multiplication by $\deg \psi$, we see that c divides $\deg \psi$. Now let φ be an element of minimal degree in $\mathrm{Hom}(E', E)$. Since E does not have CM, there exists some non-zero $m \in \mathbb{Z}$ such that $\psi = m\varphi$. Then the map $\overline{\pi} \coloneqq \varphi \circ \pi'\colon X_0(N) \to E$ is again a modular parametrization of E. Clearly such a parametrization has Manin constant equal to c/m. The same computations of $L(E,1)$ that led us to (2.3) can be performed using $\overline{\pi}\colon X_0(N) \to E$, leading us this time to:

$$L(E,1) = \frac{m \cdot M' \cdot \Omega_E}{c \cdot |E(\mathbb{Q})_{\mathrm{tors}}|} \tag{2.4}$$

for some other $M' \in \mathbb{Z}$. Both (2.3) and (2.4) give us an integral multiple of the same rational number:

$$L(E,1) = \frac{\Omega_E \cdot v}{c \cdot |E(\mathbb{Q})_{\mathrm{tors}}|} \text{ for some } v \in \mathbb{Z}.$$

This argument shows that for our purpose we can assume that $\psi = \varphi$. Now we can proceed in the following way: first we compute the curves $E_1, \ldots, E_n$ in the $\mathbb{Q}$-isogeny class of E; then for each $i = 1, \ldots, n$ we set $s_i \coloneqq \min\{\deg \varphi\colon \varphi \in \mathrm{Hom}_{\mathbb{Q}}(E_i, E)\}$ and finally we let $s \coloneqq \gcd(s_i\colon i = 1, \ldots, n)$. Since, as we said above, c divides $\deg \psi$, then c divides s. Therefore we get that

$$\frac{L(E,1)}{\Omega_E} = \frac{v}{s \cdot |E(\mathbb{Q})_{\mathrm{tors}}|} \text{ for some } v \in \mathbb{Z}. \tag{2.5}$$

Equation (2.5) has two immediate applications. The first one is the following: assume that $L(E,1) \neq 0$ and that we want to compute the L-ratio $\dfrac{L(E,1)}{\Omega_E}$. This is a rational number of which we know a multiple of the denominator, namely $s \cdot |E(\mathbb{Q})_{\mathrm{tors}}|$. Now recall the following elementary lemma.

Lemma 2.1.4. Let $B \in \mathbb{N}_{>1}$. Then for every $x \in \mathbb{R}$ there exists at most one $p/q \in \mathbb{Q}$ with q a positive divisor of B such that $|x - p/q| < \dfrac{1}{2B}$.

Proof. Let p/q and r/s be two distinct rational numbers such that q, s are positive divisors of B. Let $l = \mathrm{lcm}(q, s)$, so that $l \leq B$. Then

$$\left|\frac{p}{q} - \frac{r}{s}\right| = \frac{|p \cdot (l/q) - r \cdot (l/s)|}{l} \geq \frac{1}{B}.$$

This shows that inside an open interval of length $1/B$ there is at most one rational number with the denominator dividing B, and the claim follows. □

Notice that the bound given in the lemma is sharp, since if $x = \dfrac{3}{2B}$, then $|x - 1/B| = |x - 2/B| = 1/(2B)$.

By equation (2.5), the L-ratio $\dfrac{L(E,1)}{\Omega_E}$ is a rational number whose denominator divides $B \coloneqq s \cdot |E(\mathbb{Q})_{\mathrm{tors}}|$. Suppose that one can numerically compute $\dfrac{L(E,1)}{\Omega_E}$ within a sufficiently high precision. Let x be the approximate value found; the exact value of $\dfrac{L(E,1)}{\Omega_E}$ is by the above lemma the unique rational number of the form $\lfloor x \rfloor + A/B$ where $A \in \mathbb{Z}$ is such that $|A| < B$ and such that $\left| x - \left(\lfloor x \rfloor + \dfrac{A}{B} \right) \right| < \dfrac{1}{2B}$. Equivalently, A is the unique integer such that

$$|B(x - \lfloor x \rfloor) - A| < \frac{1}{2}.$$

The second application is the following: suppose that we can compute $L(E,1)$, finding 0 within a given precision. How can we decide whether the value is exactly 0 or a very small non-zero number? Equation 2.5 tells us that if $L(E,1) \neq 0$ then

$$|L(E,1)| \geq \frac{\Omega_E}{s \cdot |E(\mathbb{Q})_{\mathrm{tors}}|}. \tag{2.6}$$

Therefore if we find numerically that $L(E,1) < \dfrac{\Omega_E}{s \cdot |E(\mathbb{Q})_{\mathrm{tors}}|}$, then we must have $L(E,1) = 0$. Note for this purpose one can substitute s in the equation above by $s' \coloneqq \max_i\{s_i\}$ where the s_i's are defined as above; in fact it is clear that $\deg \psi \leq s'$.

2.2 Modular abelian varieties and building blocks

Let $f = \sum_{n=1}^{+\infty} a_n q^n \in S_2(\Gamma_1(N), \varepsilon)$ be a newform. The number field generated by the Fourier coefficients of f will be denoted by F. We say that f has CM if there exists a non-trivial Dirichlet character χ such that $a_p = \chi(p)a_p$ for almost all p.

Suppose that f does not have CM. Let Γ be the set of embeddings $\gamma\colon F \to \mathbb{C}$ such that there exists a Dirichlet character χ_γ with $\gamma(a_p) = \chi_\gamma(p)a_p$ for almost all primes p. Note that χ_γ is unique if it exists because f does not have CM. It is proved in [61] that Γ is an abelian subgroup of $\mathrm{Aut}(F)$ whose fixed field F^Γ is $\mathbb{Q}(a_p^2/\varepsilon(p))$ where p runs over a set S of primes not dividing N and having density 1.

Definition 2.2.1. The number field $L \coloneqq \overline{\mathbb{Q}}^{\cap_\gamma \ker \chi_\gamma}$ is called the *splitting field* of f.

The abelian variety A_f attached to f is $\mathbb{Q}$-simple and has dimension equal to $[F\colon \mathbb{Q}]$; moreover F is isomorphic to $\mathrm{End}^0_{\mathbb{Q}}(A_f)$ via the map that associates a_n to T_n and $\varepsilon(d)$ to $\langle d \rangle$ for all primes $d \in (\mathbb{Z}/N\mathbb{Z})^*$. It is proved in [30] that the splitting field of f is the smallest field over which all endomorphisms of A_f are defined. The abelian variety A_f is isogenous over L to the power of an absolutely simple abelian variety B_f, called a *building block* of A_f. The dimension of a building block satisfies the equality

$\dim B_f = t \cdot [F^\Gamma : \mathbb{Q}]$ where t is the *Schur index* of A_f; it can be either 1 or 2 depending on the splitting of the class in $H^2(F/F^\Gamma, F^*)$ of the 2-cocycle

$$c\colon \mathrm{Gal}(F/F^\Gamma) \times \mathrm{Gal}(F/F^\Gamma) \to F^*$$

$$(\sigma, \tau) \mapsto \frac{g(\chi_\sigma^{-1}) g({}^\sigma\chi_\tau^{-1})}{g(\chi_{\sigma\tau}^{-1})}$$

where $g(\chi) = \sum_{a=1}^{M} \chi(a) e^{\frac{2\pi i a}{M}}$ for a Dirichlet character χ with conductor M. From now on, we will always assume that B_f is an elliptic curve without CM, since this is the only case that we will deal with. This means that $F^\Gamma = \mathbb{Q}$, $F/\mathbb{Q}$ is abelian and the class of c is trivial in $H^2(F/\mathbb{Q}, F^*)$. The curve B_f is a $\mathbb{Q}$-curve. The number field L is the smallest one over which all endomorphisms of A_f are defined, and B_f is L-isogenous to all its Galois conjugates. Since the class of c in $H^2(F/\mathbb{Q}, F^*)$ is trivial, there exists a splitting map $\beta\colon \mathrm{Gal}(F/\mathbb{Q}) \to F^*$ such that $c(\sigma, \tau) = \dfrac{\beta(\sigma) {}^\sigma\beta(\tau)}{\beta(\sigma\tau)}$. The map β is not unique: any other splitting map differs from β by a coboundary; if β' is another splitting map then for some $a \in F^*$ we have $\beta'(\sigma) = \beta(\sigma) {}^\sigma a / a$. After having identified $H^0(J_1(N), \Omega^1_{\mathbb{C}})$ with $S_2(\Gamma_1(N))$ by pulling back via the composed map $\mathcal{H}^* \to X_1(N) \to J_1(N)$, the construction of the variety A_f as a quotient of $J_1(N)$ induces an isomorphism

$$H^0(A_f, \Omega^1_{\mathbb{C}}) \xrightarrow{\sim} \bigoplus_{\sigma\colon F \hookrightarrow \mathbb{C}} \mathbb{C} \cdot {}^\sigma f(q) \frac{dq}{q}.$$

From now on we will identify these two spaces and $H^0(A_f, \Omega^1_{\mathbb{C}})$ will be regarded as a subspace of $H^0(X_1(N), \Omega^1_{\mathbb{C}}) \simeq H^0(J_1(N), \Omega^1_{\mathbb{C}})$. Now fix a splitting map β for c. Then the following theorem holds:

Theorem 2.2.2 ([30])**.** There exists an endomorphism $w_\beta \in \mathrm{End}_L(A_f)$ such that:

1. the abelian variety $B = w_\beta(A_f)$ is a building block of A_f;
2. if ω_B is a generator of $H^0(B, \Omega^1_{\mathbb{C}})$, then $w_\beta^*(\omega_B)$ belongs to the subspace of $H^0(A_f, \Omega^1_{\mathbb{C}})$ generated by
$$\sum_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \frac{g(\chi_\sigma^{-1})}{\beta(\sigma)} {}^\sigma f;$$
3. all building blocks are of the form $a(B)$ for $a \in F$.

Let

$$\lambda = \sum_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \frac{g(\chi_\sigma^{-1})}{\beta(\sigma)} \in \mathbb{C}.$$

This quantity is non-zero (see [30, Lemma 3.1]). Then the normalized cuspform attached to (E, π) is

$$h_{w_\beta} \coloneqq \frac{1}{\lambda}(w_\beta^*(\omega)) \coloneqq \sum_{n=1}^{+\infty} \lambda_n q^n \in S_2(\Gamma_1(N)).$$

It is proved in [30] that $\lambda_n \in L$ for all n.

2.3 Quadratic $\mathbb{Q}$-curves

Definition 2.3.1. A $\mathbb{Q}$-curve E is called a *quadratic $\mathbb{Q}$-curve* if it has a model over a quadratic number field K.

From now on, E will denote a quadratic $\mathbb{Q}$-curve without CM completely defined over $K = \mathbb{Q}(\sqrt{d})$, for d a square-free integer different from 1. Let Δ_K be the discriminant of K, let $\mathrm{Gal}(K/\mathbb{Q}) := \{1, \nu\}$ and let $\mu\colon E \to {}^{\nu}E$ be a K-isogeny. Finally, let ${}^{\nu}\mu\mu$ coincide with multiplication by $m \in \mathbb{Z}$.

Lemma 2.3.2 (Serre)**.** If $\Delta_K < 0$, then $m > 0$.

Proof. Fix an embedding $K \hookrightarrow \mathbb{C}$, so that ν is the restriction of complex conjugation to K. If $\Lambda \subseteq \mathbb{C}$ is a lattice uniformizing E, the conjugate curve ${}^{\nu}E = \overline{E}$ is uniformized by $\overline{\Lambda}$. The map μ_ν can be identified with multiplication on $\mathbb{C}$ by some complex α. Thus ${}^{\nu}\mu$ is multiplication by $\overline{\alpha}$, and therefore $m = \alpha\overline{\alpha} > 0$. □

We will exhibit in section 2.9 explicit examples of $\mathbb{Q}$-curve defined over real quadratic fields with positive and negative m and of $\mathbb{Q}$-curves defined over imaginary quadratic fields, which necessarily have positive m.

Let $B = \mathrm{Res}_{K/\mathbb{Q}}(E)$ denote the restriction of scalars of E. This is an abelian surface defined over $\mathbb{Q}$, so either B is isogenous to a product of two elliptic curves, or it is a $\mathbb{Q}$-simple abelian variety. In the latter case, thanks to Theorem 1.2.3, it follows that B is isogenous to A_f for some newform f whose Fourier coefficients generate a quadratic field. It is clear from the proof of the theorem that $\mathrm{End}^0_{\mathbb{Q}}(B)$ is isomorphic to $\mathbb{Q}[x]/(x^2 - m)$, so that B is simple over $\mathbb{Q}$ precisely when m is not a square. If m is a square, the following lemma describes the structure of B up to isogeny.

Lemma 2.3.3. Suppose E is K-isogenous to an elliptic curve E_0 defined over $\mathbb{Q}$. Then $\mathrm{Res}_{K/\mathbb{Q}} E$ is isogenous over $\mathbb{Q}$ to $E_0 \times E_0^{(d)}$, where $E_0^{(d)}$ is the quadratic twist of E by d.

Proof. It is enough to check that $V_l(\mathrm{Res}_{K/\mathbb{Q}} E)$ is isomorphic as a $G_{\mathbb{Q}}$-module to $V_l(E_0 \times E_0^{(d)}) \simeq V_l(E_0) \times V_l(E_0^{(d)})$ for some prime l, where $T_l(A)$ is the l-adic module of an abelian variety A and $V_l(A) = T_l(A) \otimes \mathbb{Q}_l$. Choose as l a prime not dividing $d\Delta_{E_0}$, where Δ_{E_0} is the discriminant of E_0. By [52, p. 178], $V_l(\mathrm{Res}_{K/\mathbb{Q}} E)$ is isomorphic as a $G_{\mathbb{Q}}$-module to $\mathbb{Q}_l[G_{\mathbb{Q}}] \otimes_{\mathbb{Q}_l[G_K]} V_l(E)$, where $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Since E is K-isogenous to E_0, $V_l(E)$ is isomorphic to $V_l(E_0)$ as a G_K-module. Thus it is enough to prove that $\mathbb{Q}_l[G_{\mathbb{Q}}] \otimes_{\mathbb{Q}_l[G_K]} V_l(E_0)$ is isomorphic as a $G_{\mathbb{Q}}$-module to $V_l(E_0) \times V_l(E_0^{(d)})$. This can be easily done by looking at characters: finite dimensional Galois representations in characteristic 0 are uniquely determined up to isomorphism by their characters. Moreover, if $X \subseteq G_{\mathbb{Q}}$ is a dense subset, the character of a Galois representation is uniquely determined by its restriction to X. For every rational prime $p \nmid dl\Delta_{E_0}$, choose an arithmetic Frobenius element $\mathrm{Fr}_p \in G_{\mathbb{Q}}$ lying over it, and let X be the set of all such elements. Then X is dense in $G_{\mathbb{Q}}$. Now one checks easily that the trace of Fr_p acting on $V_l(E_0) \times V_l(E_0^{(d)})$ is given by $a_p + \left(\frac{d}{p}\right) a_p$, where $\left(\frac{d}{p}\right)$ is the Legendre symbol. On the other hand one can use the formula for the character of the induced representation to check that this equals the trace of Fr_p acting on the induced module $\mathbb{Q}_l[G_{\mathbb{Q}}] \otimes_{\mathbb{Q}_l[G_K]} V_l(E_0)$. □

In the case described above, we have

$$L(E/K, s) = L(E_0/\mathbb{Q}, s)L(E_0^{(d)}/\mathbb{Q}, s),$$

so that

$$L(E/K, 1) = L(E_0/\mathbb{Q}, 1) \cdot L(E_0^{(d)}/\mathbb{Q}, 1)$$

and we can use the method of section 2.1 to get an analogue for (2.5).

Example 2.3.4. To get an example of such a situation, start with an elliptic curve $E/\mathbb{Q}$ without CM such that the group $E(\mathbb{Q})[2]$ has order 2. Let P be its generator. Then the other two 2-torsion points P_1, P_2 will be defined over some quadratic extension $K/\mathbb{Q}$. Now let ϕ_i be the isogeny with kernel $\{O, P_i\}$ for $i = 1, 2$ and let $E_i = E/\ker\phi_i$. The curves E_1, E_2 are defined over K and $E_2 = {}^{\sigma}E_1$, since $\ker\phi_1$ and $\ker\phi_2$ are Galois conjugate one to each other. Clearly there is an isogeny $\phi = \phi_2 \circ \widehat{\phi_1} \colon E_1 \to E_2$ which has degree 4 and is defined over K. Thus the curve E_1 is a $\mathbb{Q}$-curve defined over K but isogenous to an elliptic curve defined over $\mathbb{Q}$, namely E. For an explicit example, consider the elliptic curve $E\colon y^2 = (x-1)(x^2+1)$. One checks that $j(E) = 128$, thus E has no CM. Using the notation above we have $P = (1, 0)$, $P_1 = (i, 0)$ and $P_2 = (-i, 0)$. Then E_1 is the elliptic curve defined over $\mathbb{Q}(i)$ with equation

$$E_1\colon y^2 = x^3 - x^2 + (10i + 11)x + 6i - 23.$$

2.4 The newform attached to E

From now on, we will assume that m is not a perfect square. Let

$$f = \sum_{n=1}^{+\infty} a_n q^n \in S_2(\Gamma_1(N), \varepsilon)$$

be a newform such that $\mathrm{Res}_{K/\mathbb{Q}}(E) = B$ is isogenous to A_f. The number field generated by the a_n's will be denoted by $F = \mathbb{Q}(\sqrt{m})$. Note that all endomorphisms of A_f are defined over K because μ itself is, so $\mathrm{End}^0(A_f) = \mathrm{End}^0_K(A_f)$. On the other hand, since $\mathrm{End}^0_{\mathbb{Q}}(A_f) \simeq F$, it follows that K is the splitting field of f. Following the convention of [30], we will implicitly fix an embedding of F into $\mathbb{C}$. Let $\mathrm{Gal}(F/\mathbb{Q}) = \{1, \sigma\}$. Then there exists a unique Dirichlet character χ such that ${}^{\sigma}a_p = \chi(p)a_p$ for all primes $p \nmid N$ (see [30]). The field K equals $\overline{\mathbb{Q}}^{\ker\chi}$, which implies that χ is the primitive quadratic character corresponding to K via class field theory. This means that if Δ_K is the discriminant of K then χ is the primitive quadratic character modulo $|\Delta_K|$ given by:

$$\chi(p) = \begin{cases} 1 & \text{if } p \text{ splits in } K \\ -1 & \text{if } p \text{ is inert in } K \\ 0 & \text{if } p \text{ ramifies in } K. \end{cases}$$

Now recall that for the coefficients of f it holds (see for example [60]) that $a_p = \overline{a_p}\varepsilon(p)$ for all primes $p \nmid N$. If F is quadratic real, ε must be trivial since f does not have CM. If F is quadratic imaginary, we have ${}^{\sigma}a_p = \chi(p)a_p$ but ${}^{\sigma}a_p = \overline{a_p}$ and therefore we get $\chi = \varepsilon^{-1} = \varepsilon$ as characters modulo N. Of course ε needs not to be primitive, but it is defined modulo N and $d_{K/\mathbb{Q}}$ divides N (see equation (2.9) below). Thus ε is just the composition of χ with the projection $(\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/|\Delta_K|\mathbb{Z})^*$. In order to find the q-expansion of f, we will look at local factors of the L-functions.

2.4.1 Local factors of L-functions

Let λ be a finite place of F, and let l be its residue characteristic. Let V_l be the l-adic Tate module of A_f; this is a free module of rank 2 over the ring $\mathbb{Q}_l \otimes_{\mathbb{Q}} F$ with an action of $G_{\mathbb{Q}}$. We consider

$$V_\lambda = F_\lambda \otimes_{\mathbb{Q}_l} V_l;$$

this is a 2-dimensional F_λ-linear representation of $G_{\mathbb{Q}}$.

Let p be a prime number different from l, and let D_p and I_p be a decomposition group at p and the corresponding inertia group, respectively. Let $(V_\lambda)_{I_p}$ be the space of coinvariants of V_λ under I_p.

The L-factor of f at p is of the form

$$L_p(f,s) = P_p(f,p^{-s})$$

where

$$P_p(f,x) = 1 - a_p x + \varepsilon(p) p x^2 \in F[x].$$

and we let $\varepsilon(p) = 0$ if $p \mid N$. Then we have

$$\det_{F_\lambda}(\mathrm{id} - x \cdot \mathrm{Fr}_p \mid (V_\lambda)_{I_p}) = P_p(f,x) \tag{2.7}$$

(see for example [63, Theorem 4] and [10]).

On the other hand, for every prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ lying over a rational prime p and every prime $l \neq p$, the absolute Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$ acts on the l-adic Tate module V_l of E yielding a 2-dimensional l-adic Galois representation of G_K. Let $D_\mathfrak{p} \subseteq G_K$ denote a decomposition group at $\mathfrak{p}$, $I_\mathfrak{p}$ the corresponding inertia subgroup and $\mathrm{Fr}_\mathfrak{p} \in D_\mathfrak{p}$ any Frobenius element at $\mathfrak{p}$. Then if E has good reduction at $\mathfrak{p}$ the characteristic polynomial of $\mathrm{Fr}_\mathfrak{p}$ is given by

$$P_\mathfrak{p}(E,x) = 1 - c_\mathfrak{p} x + N_{K/\mathbb{Q}}(\mathfrak{p}) x^2 \in \mathbb{Z}[x],$$

where $c_\mathfrak{p} = N_{K/\mathbb{Q}}(\mathfrak{p}) + 1 - |E(\mathbb{F}_\mathfrak{p})|$. If E has bad reduction at $\mathfrak{p}$, we set

$$P_\mathfrak{p}(E,x) = \begin{cases} 1 & \text{if } E \text{ has additive reduction} \\ 1-x & \text{if } E \text{ has split multiplicative reduction} \\ 1+x & \text{if } E \text{ has non-split multiplicative reduction.} \end{cases}$$

The L-factor at $\mathfrak{p}$ is given by

$$L_\mathfrak{p}(E,s) = P_\mathfrak{p}(E, N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}).$$

The following equation holds for all $\mathfrak{p}$:

$$\det_{\mathbb{Q}_l}(\mathrm{id} - x \cdot \mathrm{Fr}_\mathfrak{p} \mid (V_l)_{I_\mathfrak{p}}) = P_\mathfrak{p}(E,x).$$

By [52, Proposition 3] and [63, Theorem 5], the following equalities hold for all rational primes p:

$$\prod_{\mathfrak{p}\mid p} L_\mathfrak{p}(E/K,s) = L_p(A_f/\mathbb{Q},s) = \prod_{\vartheta \in \mathrm{Gal}(F/\mathbb{Q})} L_p({}^\vartheta f, s), \tag{2.8}$$

where $L_p(A_f/\mathbb{Q}, s)$ is the local factor at p of L-function attached to the Galois representation on the l-adic Tate module of A_f.

The equality (2.8) will be used to compute the a_p's. In order to do that, we will separately analyze primes of good and bad reduction for E. According to [52, Proposition 1], if $\mathcal{N}_K(E)$ is the conductor of E, then one has that

$$N_{K/\mathbb{Q}}(\mathcal{N}_K(E))\Delta_K^2 = \mathcal{N}_{\mathbb{Q}}(\mathrm{Res}_{K/\mathbb{Q}}(E))$$

and combining this with the fact that $\mathcal{N}_{\mathbb{Q}}(A_f) = N^2$ (see [11]) we get the following formula:

$$N_{K/\mathbb{Q}}(\mathcal{N}_K(E))\Delta_K^2 = N^2. \tag{2.9}$$

Therefore primes of bad reduction for A_f are exactly primes lying under primes of bad reduction for E and primes which ramify in K.

Lemma 2.4.1. The conductor of E is a principal ideal generated by an integer. Moreover, E has bad reduction at a prime $\mathfrak{p}$ if and only if it has bad reduction at ${}^{\nu}\mathfrak{p}$.

Proof. Let $\mathcal{N}_K(E) = \mathfrak{p}^r I$, where $\mathfrak{p}$ is a prime ideal of K, $r \in \mathbb{N}$ and I is an ideal of K which is coprime with $\mathfrak{p}$. We will show that either $\mathfrak{p}^r$ is a principal ideal generated by p^k for some k, where p is the rational prime lying under $\mathfrak{p}$, or ${}^{\nu}\mathfrak{p}^r$ exactly divides I.

Suppose that $\mathfrak{p}$ lies above a ramified rational prime p. Then $N_{K/\mathbb{Q}}(\mathfrak{p}) = p$. Since $\mathfrak{p}$ is the only prime lying above p and equation (2.9) implies that $N_{K/\mathbb{Q}}(\mathcal{N}_K(E))\Delta_K^2$ must be a square in $\mathbb{Z}$, this means that $\mathfrak{p}$ has to divide the conductor of E an even number of times, say $2k$ times. This implies $r = 2k$ and $\mathfrak{p}^r = (p^k)$.

Suppose now that $\mathfrak{p}$ lies over an inert prime p. This amounts to saying that $\mathfrak{p} = (p)$, implying that $\mathfrak{p}^r = (p)^r$.

Finally, suppose that $\mathfrak{p}$ lies over a split prime p. Since E is K-isogenous to ${}^{\nu}E$, the two curves have the same conductor. But $\mathcal{N}_K({}^{\nu}E) = {}^{\nu}\mathcal{N}_K(E)$ and this implies that ${}^{\nu}\mathfrak{p}^r$ exactly divides $\mathcal{N}_K({}^{\nu}E)$ and hence also $\mathcal{N}_K(E)$, concluding the proof. □

Thanks to the above lemma, by a small abuse of notation we can say that E has bad (good) reduction at a rational prime p.

2.4.2 Primes of good reduction for E

Let p be a prime of good reduction for E. Equation (2.8) becomes:

$$\prod_{\mathfrak{p}|p}(1 - c_{\mathfrak{p}}N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{1-2s}) = (1 - a_p p^{-s} + \varepsilon(p)p^{1-2s})(1 - {}^{\sigma}a_p p^{-s} + {}^{\sigma}\varepsilon(p)p^{1-2s}). \tag{2.10}$$

Ramified case

Suppose p is a rational prime ramified in K. In this case, p divides N because of (2.9), and equation (2.10) therefore becomes

$$1 - c_{\mathfrak{p}}p^{-s} + p \cdot p^{-2s} = 1 - (a_p + {}^{\sigma}a_p)p^{-s} + (a_p \cdot {}^{\sigma}a_p)p^{-2s},$$

where $\mathfrak{p}$ is the unique prime of K lying over p. We then have

$$\begin{cases} a_p + {}^{\sigma}a_p = c_{\mathfrak{p}} \\ a_p \cdot {}^{\sigma}a_p = p, \end{cases}$$

implying

$$a_p = \frac{c_{\mathfrak{p}} \pm \sqrt{c_{\mathfrak{p}}^2 - 4p}}{2}.$$

In particular, $c_{\mathfrak{p}} - 4p$ is a square in F.

Inert case

If p is inert in K and $\mathfrak{p}$ is the unique prime lying above it, we get

$$1 - c_{\mathfrak{p}} p^{-2s} + p^{2-4s} = 1 - (a_p + {}^{\sigma}a_p)p^{-s} + (2\varepsilon(p)p + a_p \cdot {}^{\sigma}a_p)p^{-2s} + \\ + (a_p + {}^{\sigma}a_p)p \cdot p^{-3s} + p^{2-4s},$$

which leads to the following system:

$$\begin{cases} a_p + {}^{\sigma}a_p = 0 \\ 2\varepsilon(p)p + a_p \cdot {}^{\sigma}a_p = -c_{\mathfrak{p}}. \end{cases}$$

Thus $a_p = \pm\sqrt{c_{\mathfrak{p}} + 2\varepsilon(p)p}$ and in particular $c_{\mathfrak{p}} + 2\varepsilon(p)p$ is a square in F. Here $\varepsilon(p) = 1$ if F is real and $\varepsilon(p) = -1$ if F is imaginary.

Split case

If p is split in K, then $\varepsilon(p) = 1$, there are two primes $\mathfrak{p}_1, \mathfrak{p}_2$ lying over p and $\mathfrak{p}_2 = {}^{\nu}\mathfrak{p}_1$. Let l be a prime different from p. Since E and ${}^{\nu}E$ are isogenous, the two Tate modules $T_l(E)$ and $T_l({}^{\nu}E)$ are isomorphic as G_K-modules. This shows that $c_{\mathfrak{p}_i}(E) = c_{\mathfrak{p}_i}({}^{\nu}E)$ for $i = 1, 2$. Now we claim that $c_{\mathfrak{p}_1}(E) = c_{\mathfrak{p}_2}({}^{\nu}E)$. To see this, let $\overline{\nu} \in G_{\mathbb{Q}}$ be any lift of ν, and let

$$c_{\overline{\nu}} \colon G_K \to G_K$$
$$\tau \mapsto \overline{\nu}\tau\overline{\nu}^{-1}$$

be the conjugation by $\overline{\nu}$. This is a well-defined homomorphism because G_K is normal in $G_{\mathbb{Q}}$. Now let

$$\varphi_{\overline{\nu}} \colon \operatorname{Aut}(T_l(E)) \to \operatorname{Aut}(T_l({}^{\nu}E))$$
$$f \mapsto (x \mapsto {}^{\overline{\nu}}f({}^{\overline{\nu}^{-1}}x)).$$

Then it is easy to check that the following diagram commutes:

$$\begin{array}{ccc} G_K & \xrightarrow{\quad c_{\nu} \quad} & G_K \\ \downarrow & & \downarrow \\ \operatorname{Aut}(T_l(E)) & \xrightarrow{\varphi_{\overline{\nu}}} & \operatorname{Aut}(T_l({}^{\nu}E)) \end{array}$$

where the two vertical arrows are the usual l-adic representations of G_K. If $\mathrm{Fr}_{\mathfrak{p}_i} \in G_K$ is a Frobenius at $\mathfrak{p}_i$ for $i = 1, 2$, it is clear that $c_{\overline{\nu}}(\mathrm{Fr}_{\mathfrak{p}_1}) = \mathrm{Fr}_{\mathfrak{p}_2}$. On the other hand, if one chooses a $\mathbb{Z}_l$-basis $\{\mathbf{e_1}, \mathbf{e_2}\}$ for $T_l(E)$, then $\{{}^{\overline{\nu}}\mathbf{e_1}, {}^{\overline{\nu}}\mathbf{e_2}\}$ is a $\mathbb{Z}_l$-basis for $T_l({}^{\nu}E)$ and the map $\varphi_{\overline{\nu}}$ written with respect to these bases is just the identity. This shows that the characteristic polynomial of $\mathrm{Fr}_{\mathfrak{p}_1}$ acting on $T_l(E)$ coincides with the characteristic polynomial of $\mathrm{Fr}_{\mathfrak{p}_2}$ acting on $T_l({}^{\nu}E)$, and the claim follows.

By the discussion above, we have that $c_{\mathfrak{p}_1}(E) = c_{\mathfrak{p}_2}(E)$, so that we can just write $c_{\mathfrak{p}}$ for that. Equation (2.10) reads:

$$(1 - c_{\mathfrak{p}}p^{-s} + p^{1-2s})^2 = (1 - a_p p^{-s} + p^{1-2s})(1 - {}^{\sigma}a_p p^{-s} + p^{1-2s}),$$

leading to

$$\begin{cases} a_p + {}^{\sigma}a_p = 2c_{\mathfrak{p}} \\ a_p \cdot {}^{\sigma}a_p = c_{\mathfrak{p}}^2. \end{cases}$$

Therefore $a_p = c_{\mathfrak{p}}$ and ${}^{\sigma}a_p = a_p$.

2.4.3 Primes of bad reduction for E

Let p be a prime of bad reduction for E. Then $\varepsilon(p) = 0$. Equation (2.8) becomes:

$$\prod_{\mathfrak{p}|p}(1 - c_{\mathfrak{p}}N(\mathfrak{p})^{-s}) = \prod_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})}(1 - {}^{\sigma}a_p p^{-s}), \tag{2.11}$$

where $c_{\mathfrak{p}} = 1, -1, 0$ if E has split multiplicative, non-split multiplicative or additive reduction at $\mathfrak{p}$, respectively.

Ramified case

Let $\mathfrak{p}$ be the unique prime lying above p. In the proof of Lemma 2.4.1, we showed that $\mathfrak{p}$ has to divide the conductor of E an even number of times, and so the reduction at $\mathfrak{p}$ must be additive. This implies $c_{\mathfrak{p}} = a_p = 0$.

Inert case

Let p be inert in K and let $\mathfrak{p}$ be the unique prime lying above p. Then

$$1 - c_{\mathfrak{p}}p^{-2s} = 1 - (a_p + {}^{\sigma}a_p)p^{-s} + a_p \cdot {}^{\sigma}a_p p^{-2s}.$$

Therefore $a_p = c\sqrt{m}$ for some $c \in \mathbb{Z}$ and $c^2 m = c_{\mathfrak{p}}$. Since $|c_{\mathfrak{p}}| \leq 1$, if $|m| > 1$, then we must have $c_{\mathfrak{p}} = a_p = c = 0$. Otherwise, namely if $m = -1$, we must have either $c_{\mathfrak{p}} = a_p = c = 0$ or $c_{\mathfrak{p}} = -1$, $c \in \{\pm 1\}$ and $a_p = c\sqrt{-1}$.

Split case

Let $\mathfrak{p}_1, \mathfrak{p}_2$ be the primes lying above p. The same argument we used for the split case applies again, just noticing that since $T_l(E) \simeq T_l({}^{\nu}E)$ as G_K-modules, we have $T_l(E)_{I_{\mathfrak{p}_1}} \simeq T_l({}^{\nu}E)_{I_{\mathfrak{p}_1}}$ as $D_{\mathfrak{p}_1}$-modules, where $D_{\mathfrak{p}_1} \subseteq G_K$ is any decomposition group for $\mathfrak{p}_1$. Therefore we get $c_{\mathfrak{p}_1} = c_{\mathfrak{p}_2}$ and consequently

$$1 - 2c_{\mathfrak{p}_1}p^{-s} + c_{\mathfrak{p}_1}^2 p^{-2s} = 1 - 2a_p p^{-s} + {}^{\sigma}a_p \cdot a_p p^{-2s},$$

so that $a_p = c_{\mathfrak{p}_1} = c_{\mathfrak{p}_2}$.

2.4.4 Finding the sign of the a_p's

Now given E, we have to decide for each p which coefficient to choose between a_p and ${}^{\sigma}a_p$ when p is a ramified or inert prime of good reduction for E or, when $m = -1$, p is inert and E has non-split multiplicative reduction at p. The ambiguity arises from the fact that, unlike in the setting of elliptic curves over $\mathbb{Q}$ to which we can associate a unique newform, here we associate to E a pair of conjugate newforms, which a priori we cannot distinguish one from another. The object we can easily compute starting from E is a family of pairs $\{(a_p, {}^{\sigma}a_p)\}_p$. We will see that the choice of a square root of m will allow us to pick, for every prime p, exactly one between a_p and ${}^{\sigma}a_p$ so that the collection of all the picked coefficients will coincide with the collection of the Fourier coefficients of prime index of a newform f. Choosing the other square root of m will give us the Fourier coefficients of ${}^{\sigma}f$. To start, recall that $F = \mathbb{Q}(a_n \colon n \in \mathbb{N}) = \mathbb{Q}(\sqrt{m})$ acts on B, where for every prime p the coefficient a_p acts as T_p does. Note that $\mu \colon E \to {}^{\nu}E$ induces an endomorphism $\mu_* \colon B \to B$ such that $({}^{\nu}\mu)_* \circ \mu_* = m$. Furthermore, we have $({}^{\nu}\mu)_* = \mu_*$. Therefore the choice of a square root of m induces an inclusion $\mathbb{Z}[\mu_*] \subseteq F$. From now on, we fix such an embedding. This will correspond to the choice of one newform in the Galois orbit of f. Now note that the ring $\mathrm{End}_K(B_K)$ can be identified with the ring $\begin{pmatrix} \mathrm{End}_K(E) & \mathrm{Hom}_K({}^{\nu}E, E) \\ \mathrm{Hom}_K(E, {}^{\nu}E) & \mathrm{End}_K({}^{\nu}E) \end{pmatrix}$, whose elements are 2×2 matrices (a_{ij}) whose entries lie in the corresponding set of isogenies; for example, $a_{11} \in \mathrm{End}_K(E)$. Under this identification, the subring $\mathbb{Z}[\mu_*]$ corresponds to the subring $\mathbb{Z} \cdot \begin{pmatrix} 0 & {}^{\nu}\mu \\ \mu & 0 \end{pmatrix}$.

Before starting to analyze each problematic case, let us recall two fundamental facts. If l is any prime, then:

i) there is a canonical isomorphism of $\mathbb{Z}_l[G_{\mathbb{Q}}]$-modules

$$T_l(B) \simeq T_l(E) \otimes_{\mathbb{Z}_l[G_K]} \mathbb{Z}_l[G_{\mathbb{Q}}] \tag{2.12}$$

(see [52]);

ii) let p be a prime different from l. Then there is an isomorphism of $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$-modules

$$(T_l(B))^{I_p} \to T_l(B_{\mathbb{F}_p}) \tag{2.13}$$

(see for example [67]).

Inert primes of good reduction

Let p be an inert prime of good reduction for E, and let $\mathfrak{p}$ be the unique prime of K lying above p. In view of (2.9), B has good reduction at p. Now fix a prime $l \neq p$. Then the Tate module $T_l(B)$ is unramified at p. Since F acts $\mathbb{Q}_l$-linearly on $T_l(B)$, the Tate module is also a $F \otimes \mathbb{Q}_l$-module, and one can show that $T_l(B)$ has dimension 2 as an $F \otimes \mathbb{Q}_l$-module (see for example [20]). Moreover, any Frobenius at p satisfies the equation

$$x^2 + a_p x + \varepsilon(p)p = 0$$

in $\mathrm{End}_{F \otimes \mathbb{Q}_l}(T_l(B))$, where a_p is viewed as an endomorphism of $T_l(B)$. Since $T_l(B)$ is isomorphic to $T_l(B_{\mathbb{F}_p})$ as a $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$-module, any Frobenius at p must satisfy the

same equation in $\mathrm{End}_{F\otimes\mathbb{Q}_l}(T_l(B_{\mathbb{F}_p}))$. Now note that the Frobenius at p acts on $B_{\mathbb{F}_p}$ as the matrix $\begin{pmatrix} 0 & {}^{\nu}\mathrm{Fr}_p \\ \mathrm{Fr}_p & 0 \end{pmatrix}$, where $E_{\mathfrak{p}}$ is the reduction of E modulo $\mathfrak{p}$ and $\mathrm{Fr}_p\colon E_{\mathfrak{p}} \to {}^{\nu}E_{\mathfrak{p}}$ maps (x,y) to (x^p,y^p) and ${}^{\nu}\mathrm{Fr}_p\colon {}^{\nu}E_{\mathfrak{p}} \to E_{\mathfrak{p}}$ is defined analogously. From the computations of the coefficients of f performed above, we see that there exists an integer c such that $a_p = c\sqrt{m}$, so that a_p acts on B as μ followed by multiplication by c. Therefore a_p acts on $B_{\mathbb{F}_p}$ as the matrix $\begin{pmatrix} 0 & c\,{}^{\nu}\mu_{\mathfrak{p}} \\ c\mu_{\mathfrak{p}} & 0 \end{pmatrix}$, where $\mu_{\mathfrak{p}}$ is the reduction of μ modulo $\mathfrak{p}$. Hence the following must hold:

$$\begin{pmatrix} {}^{\nu}\mathrm{Fr}_p\circ\mathrm{Fr}_p & 0 \\ 0 & \mathrm{Fr}_p\circ{}^{\nu}\mathrm{Fr}_p \end{pmatrix} - \begin{pmatrix} c\,{}^{\nu}\mu_{\mathfrak{p}}\circ\mathrm{Fr}_p & 0 \\ 0 & c\mu_{\mathfrak{p}}\circ{}^{\nu}\mathrm{Fr}_p \end{pmatrix} + \begin{pmatrix} \varepsilon(p)p & 0 \\ 0 & \varepsilon(p)p \end{pmatrix} = 0,$$

implying that

$$\mathrm{Fr}_{p^2} - c\,{}^{\nu}\mu_{\mathfrak{p}}\circ\mathrm{Fr}_p + \varepsilon(p)p = 0$$

on $E_{\mathfrak{p}}$, where Fr_{p^2} is the usual Frobenius. What we know is the absolute value of c, we have to decide the sign. Let $T = \mathrm{Fr}_{p^2} - |c|\,{}^{\nu}\mu_{\mathfrak{p}}\circ\mathrm{Fr}_p + \varepsilon(p)p$ and $S = \mathrm{Fr}_{p^2} + |c|\,{}^{\nu}\mu_{\mathfrak{p}}\circ\mathrm{Fr}_p + \varepsilon(p)p$. Let Q be a point on $E_{\mathfrak{p}}$. Note that if $T(Q) = S(Q)$ then $(S-T)(Q) = 0$, so $(2|c|\,{}^{\nu}\mu_{\mathfrak{p}}\circ\mathrm{Fr}_p)(Q) = 0$, which implies that Q has order dividing $2p|mc|$. Therefore if Q has order coprime with $2p|mc|$ then $T(Q) \neq S(Q)$. If $T(Q) = 0$ then c is positive, otherwise it is negative. This gives us an algorithm to decide the sign of c. Note that if we had fixed the other embedding $\mathbb{Z}[\mu_*] \to \mathbb{Q}(\sqrt{m})$, we would get the opposite sign.

Ramified primes of good reduction

Let now p be a ramified prime of good reduction for E, and let $\mathfrak{p}$ be the unique prime of $\mathcal{O}_K$ lying above it. Then we have the following lemma.

Lemma 2.4.2. There is an exact sequence of abelian varieties over $\mathbb{F}_p$:

$$0 \to \mathbb{G}_a \to B_{\mathbb{F}_p} \to E_{\mathfrak{p}} \to 0.$$

Proof. The proof is essentially an application of the results of [26]. In the notation of section 5 of that paper, the discrete valuation ring D is $\mathbb{Z}_{(p)}$, i.e. the localization of $\mathbb{Z}$ with respect to the prime ideal (p), while the discrete valuation ring D' is $\mathcal{O}_{K,\mathfrak{p}}$. The abelian variety X is $\mathrm{Res}_{\mathcal{O}_{K,\mathfrak{p}}/\mathbb{Z}_{(p)}}\mathcal{E}$, where $\mathcal{E}$ is the Néron model of E over $\mathcal{O}_{K,\mathfrak{p}}$. By [6, Proposition 6, section 7.6], $\mathrm{Res}_{\mathcal{O}_{K,\mathfrak{p}}/\mathbb{Z}_{(p)}}\mathcal{E}$ is the Néron model of B over $\mathbb{Z}_{(p)}$, which we denote by $\mathcal{B}$. Now again in [26, section 5.2], the author constructs a filtration $\mathcal{B}_{\mathbb{F}_p} = F^0\mathcal{B}_{\mathbb{F}_p} \supseteq F^1\mathcal{B}_{\mathbb{F}_p} \supseteq F^2\mathcal{B}_{\mathbb{F}_p} = 0$ where for any $\mathbb{F}_p$-algebra C and $i = 0,1,2$ one has

$$(F^i\mathcal{B}_{\mathbb{F}_p})(C) = \ker(\mathcal{B}_{\mathbb{F}_p}(C) \xrightarrow{\sim} \mathcal{E}(C[t]/(t^2)) \to \mathcal{E}(C[t]/(t^i))).$$

The successive quotients of the filtration $\mathrm{Gr}\,\mathcal{B}_{\mathbb{F}_p} \coloneqq F^i\mathcal{B}_{\mathbb{F}_p}/F^{i+1}\mathcal{B}_{\mathbb{F}_p}$ give rise to a short exact sequence

$$0 \to F^1\mathcal{B}_{\mathbb{F}_p} \to \mathcal{B}_{\mathbb{F}_p} \to \mathrm{Gr}^0\,\mathcal{B}_{\mathbb{F}_p} \to 0.$$

Now $\mathrm{Gr}^0\,\mathcal{B}_{\mathbb{F}_p} = \mathcal{B}_{\mathbb{F}_p}/F^1\mathcal{B}_{\mathbb{F}_p} \simeq \mathcal{E}_{\mathfrak{p}}$, while $\mathrm{Gr}^1\,\mathcal{B}_{\mathbb{F}_p} = F^1\mathcal{B}_{\mathbb{F}_p}$ by the fact that $F^2\mathcal{B}_{\mathbb{F}_p} = 0$. The isomorphism (5.1.2) in [26] tells us that

$$\mathrm{Gr}^i\,\mathcal{B}_{\mathbb{F}_p} \xrightarrow{\sim} T_{\mathcal{E}_{\mathfrak{p}},0} \otimes_{\mathbb{F}_p} (m/m^2)^{\otimes i}$$

as group schemes, where m is the maximal ideal of $\mathcal{O}_{K,\mathfrak{p}}$. This shows that $\mathrm{Gr}^0\,\mathcal{B}_{\mathbb{F}_p} \simeq \mathbb{G}_a$, proving the claim. □

By equation (2.7), we notice that a_p is the trace of Fr_p on $(V_\lambda)_{I_p} = (V_l(B) \otimes_{\mathbb{Q}_l} F_\lambda)_{I_p}$. The isomorphism (2.12) shows that we can find a basis of $T_l(B)$ such that I_p acts via matrices of the form $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & * & * \\ 0 & 0 & * & * \end{pmatrix}$. Therefore $(T_l(B))_{I_p} \simeq (T_l(B))^{I_p}$. Now the lemma above implies, since $\mathbb{G}_a$ is l-torsion free, that $(T_l(B))^{I_p} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ is a 1-dimensional F-linear representation of D_p, and therefore Fr_p acts as multiplication by a_p on $(T_l(B))^{I_p}$. Now we can use the same argument we used above, together with (2.13), to see that $\mathrm{Fr}_p \colon E_\mathfrak{p} \to {}^\nu E_\mathfrak{p}$ equals the map $c \cdot \mu_\mathfrak{p}$, where c is an integer of which we know the absolute value but not the sign. This sign can be determined in an analogous way as in the inert case.

Inert primes of multiplicative reduction

We now consider the case where p is a prime that is inert in K such that E has non-split multiplicative reduction at p. This case only occurs if $m = -1$, and we will exhibit in section 2.9 an example of a $\mathbb{Q}$-curve over $\mathbb{Q}(\sqrt{17})$ which has non-split multiplicative reduction at 5.

Let $\mathfrak{p}$ be the unique prime of K lying over p. Let G be the smooth locus of the reduction of E modulo $\mathfrak{p}$; this is a non-split torus of dimension 1 over $k(\mathfrak{p})$. Then we have a canonical isomorphism

$$B_{\mathbb{F}_p} \simeq \mathrm{Res}_{k(\mathfrak{p})/\mathbb{F}_p} G.$$

We note that reducing μ gives an isomorphism

$$\mu_\mathfrak{p} \colon G \to {}^\nu G,$$

where ${}^\nu G$ is the Galois conjugate of G via ν, which reduces to the Frobenius on $k(\mathfrak{p})$, such that if ${}^\nu\mu_\mathfrak{p} \colon {}^\nu G \to G$ is the conjugate of $\mu_\mathfrak{p}$, then we have ${}^\nu\mu_\mathfrak{p} \circ \mu_\mathfrak{p} = -1$.

The L-factor we are trying to determine is $1 - a_p p^{-s}$. Recall that in our setting, we have $a_\mathfrak{p} = -1$ and $a_p = c\sqrt{-1}$ for some unknown $c \in \{\pm 1\}$. This a_p arises as the eigenvalue of Fr_p on $(V_\lambda)_{I_p}$ by (2.7). Since E has semi-stable reduction at $\mathfrak{p}$, the inertia subgroup at $\mathfrak{p}$ acts unipotently on $V_l(E)$. Using (2.12), one can check that I_p acts unipotently on V_λ. Therefore there is a short exact sequence

$$0 \longrightarrow (V_\lambda)^{I_p} \longrightarrow V_\lambda \longrightarrow (V_\lambda)_{I_p} \longrightarrow 0.$$

The product of the eigenvalue of Fr_p on $(V_\lambda)_{I_p}$ and the eigenvalue of Fr_p on $(V_\lambda)^{I_p}$ equals $-p$, because the determinant of the Galois representation on V_λ equals χ times the l-adic cyclotomic character χ_l (see for example [60, Proposition 2.2]) and $\chi(p) = -1$ and $\chi_l(p) = p$. Therefore the eigenvalue of Fr_p on $(V_\lambda)^{I_p}$ equals $-p/a_p = -p/(c\sqrt{-1}) = cp\sqrt{-1}$. This implies that the Frobenius endomorphism Fr_p of $B_{\mathbb{F}_p}$ equals $cp(\mu_\mathfrak{p})_*$. This Fr_p is induced by the endomorphism of $G \times {}^\nu G$ defined by the matrix $\begin{pmatrix} 0 & \mathrm{Fr}_p \\ \mathrm{Fr}_p & 0 \end{pmatrix}$. Furthermore, the endomorphism $(\mu_\mathfrak{p})_*$ of $B_{\mathbb{F}_p}$ is induced by the endomorphism of $G \times {}^\nu G$ defined by the matrix $\begin{pmatrix} 0 & {}^\nu\mu_\mathfrak{p} \\ \mu_\mathfrak{p} & 0 \end{pmatrix}$. This implies that the two maps Fr_p and $cp\mu_\mathfrak{p}$ from G to ${}^\nu G$ are equal. Hence we can determine c by taking random points Q of G and checking for which c we have the equality $\mathrm{Fr}_p(Q) = cp\mu_\mathfrak{p}(Q)$ in ${}^\nu G$.

2.5 Computing $L(E,1)$

We mentioned in the previous section that there is an equality of L-functions

$$L(E/K,s) = L(f,s)\cdot L({}^{\sigma}f,s).$$

From this we can derive the formula

$$L(E/K,1) = \left(-2\pi i\int_0^{i\infty} f(t)dt\right)\cdot\left(-2\pi i\int_0^{i\infty} {}^{\sigma}f(t)dt\right). \tag{2.14}$$

The key point now is that there exists a map $\pi\colon A_f \to E$ defined over K (and consequently there exists a conjugate map ${}^{\nu}\pi\colon A_f \to {}^{\nu}E$). In fact if w_β is an endomorphism of A_f as in Theorem 2.2.2, then there is an isogeny $\varphi\colon w_\beta(B)\to E$, and we can let $\pi := w_\beta\circ\varphi$. This allows us to consider the pullback of an invariant differential ω_E on E, but this time such a pullback needs not to be a multiple of the cusp form f. In fact, in the notation of section 2.2, by Theorem 2.2.2 the space generated by $\pi^*(\omega_E)$ is spanned by $h = h_\beta$ and ${}^{\nu}h = {}^{\nu}(h_\beta)$. First of all we need to understand how to change the base of $H^0(A_f,\Omega^1_{\mathbb{C}})$ from $\{f,{}^{\sigma}f\}$ to $\{h,{}^{\nu}h\}$. This is easily done by just looking at the definitions. Recall the following standard result:

$$g(\chi) = \begin{cases}\sqrt{\Delta_K} & \text{if } \Delta_K > 0\\ i\sqrt{-\Delta_K} & \text{if } \Delta_K < 0\end{cases}$$

(for a proof see for example [42]). From now on, when we will write $\sqrt{\Delta_K}$ we will mean one of the two values given above, according to the sign of Δ_K. Set $\kappa := \dfrac{\sqrt{\Delta_K}}{\beta(\sigma)} \in FK$. Now we have to be a bit careful in distinguishing two cases, namely $K = F$ and $K \neq F$ (as we will see in section 2.9, both cases actually occur). In the first case we can identify the two Galois groups $\mathrm{Gal}(K/\mathbb{Q})$ and $\mathrm{Gal}(F/\mathbb{Q})$ so that $\nu = \sigma$. In the second one we can identify $\mathrm{Gal}(FK/\mathbb{Q})$ with the group $\{1,\sigma,\nu,\sigma\nu\}$, where by a small abuse of notation σ generates $\mathrm{Gal}(FK/K)$ and ν generates $\mathrm{Gal}(FK/F)$. Recall that according to the definition of the cocycle c given in section 2.2 we have

$$c(\sigma,\sigma) = \frac{g(\chi^{-1})g({}^{\sigma}\chi^{-1})}{g(\mathbb{1}_{\Delta_K})} = g(\chi)^2 = {}^{\sigma}\beta(\sigma)\beta(\sigma).$$

This implies $\kappa\cdot{}^{\sigma}\kappa = \eta$, where $\eta = -1$ if $K = F$ and $\eta = 1$ if $K \neq F$. Note also that in this last case ${}^{\nu}\kappa = -\kappa$. Then by definition

$$h = \frac{1}{1+\kappa}(f+\kappa{}^{\sigma}f) = \frac{(1+{}^{\sigma}\kappa)f + (\eta+\kappa){}^{\sigma}f}{(1+\kappa)(1+{}^{\sigma}\kappa)}.$$

A priori h has coefficients in the composite field FK but it is clear that as long as $\eta = 1$ one has that ${}^{\sigma}h = h$, which implies that the coefficients of h lie in fact in K, as predicted by the theory. This is trivially true in the case where $K = F$ and $\eta = -1$. One checks easily that

$$\begin{pmatrix} h \\ {}^{\nu}h\end{pmatrix} = \begin{pmatrix} \dfrac{1}{1+\kappa} & \dfrac{1}{1+\eta\cdot{}^{\sigma}\kappa} \\ \dfrac{1}{1-\kappa} & \dfrac{1}{1-\eta\cdot{}^{\sigma}\kappa}\end{pmatrix}\begin{pmatrix} f \\ {}^{\sigma}f\end{pmatrix}.$$

Note that the determinant of the transformation equals $\dfrac{2}{\kappa - \eta \cdot {}^{\sigma}\kappa}$, so it is always non-zero. Inverting the system leads to

$$\begin{pmatrix} f \\ {}^{\sigma}f \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1+\kappa & 1-\kappa \\ 1+\eta\cdot{}^{\sigma}\kappa & 1-\eta\cdot{}^{\sigma}\kappa \end{pmatrix} \begin{pmatrix} h \\ {}^{\nu}h \end{pmatrix}.$$

This gives

$$\begin{cases} L(f,1) = \dfrac{1}{2}(1+\kappa)L(h,1) + \dfrac{1}{2}(1-\kappa)L({}^{\nu}h,1) \\ L({}^{\sigma}f,1) = \dfrac{1}{2}(1+\eta\cdot{}^{\sigma}\kappa)L(h,1) + \dfrac{1}{2}(1-\eta\cdot{}^{\sigma}\kappa)L({}^{\nu}h,1) \end{cases}$$

and substituting in equation (2.14),

$$L(E/K,1) = \frac{(1+\kappa)(1+\eta\cdot{}^{\sigma}\kappa)}{4} L(h,1)^2 + \frac{(1-\kappa)(1-\eta\cdot{}^{\sigma}\kappa)}{4} L({}^{\nu}h,1)^2. \tag{2.15}$$

Note that both the element $\kappa \in FK$ and the cusp form h depend on the chosen splitting map β. We will now explain how to make a choice for the splitting map which will allows us to simplify equation (2.15).

Let β be a splitting map. Then the element $\beta(\sigma)$ satisfies $N_{F/\mathbb{Q}}(\beta(\sigma)) = \Delta_K$. This proves that $m \in N_{K/\mathbb{Q}}(K)$, so let $\alpha \in K$ be an element of norm m. Let ω_E be an invariant differential on E and let $\omega'_{{}^{\nu}E}$ be an invariant differential on ${}^{\nu}E$. Let $\vartheta \in K$ be such that $\mu^*(\omega'_{{}^{\nu}E}) = \vartheta \cdot \omega_E$ and set $\omega_{{}^{\nu}E} \coloneqq \dfrac{\vartheta}{\alpha}\omega'_{{}^{\nu}E}$. Then $\mu^*(\omega_{{}^{\nu}E}) = \alpha \cdot \omega_E$. Let now $\alpha' \in K$ be such that $({}^{\nu}\mu)^*(\omega_E) = \alpha'\omega_{{}^{\nu}E}$. Since $({}^{\nu}\mu \circ \mu)^*$ coincides with multiplication by m, this shows that $\alpha' = {}^{\nu}\alpha$. To find explicitly such an α, choose a Weierstrass equation for E of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ for some $a_1, \dots, a_6 \in K$ and then let $\omega_E = \dfrac{dx}{2y + a_1x + a_3}$ and $\omega_{{}^{\nu}E} = \dfrac{dx}{2y + {}^{\nu}a_1x + {}^{\nu}a_3}$. Then $\mu^*(\omega_{{}^{\nu}E}) = \alpha \cdot \omega_E$, where $\alpha \in K$ has norm m.

From now on, ω_E and $\omega_{{}^{\nu}E}$ will be invariant differentials on E and ${}^{\nu}E$, respectively, such that $\mu^*(\omega_{{}^{\nu}E}) = \alpha \cdot \omega_E$ where $\alpha \in K$ has norm m. Write $\alpha = p + q\sqrt{\Delta_K}$ for some $p, q \in \mathbb{Q}$ (note that $q \neq 0$ because by assumption m is not a square in $\mathbb{Q}$). Then we get a splitting map $\beta\colon \mathrm{Gal}(F/\mathbb{Q}) \to F^*$ by setting $\beta(\sigma) = \dfrac{p}{q} + \dfrac{1}{q}\sqrt{m}$, since then $N_{F/\mathbb{Q}}(\beta(\sigma)) = \Delta_K$. The splitting map β that we get in this way induces an endomorphism w of the abelian variety A_f as described in Theorem 2.2.2, and the image $w(A_f) \coloneqq B$ is isogenous to E since both B and E are building blocks of A_f. Let $\varphi\colon B \to E$ be an isogeny of minimal degree: with a little abuse of notation we will denote the composition $\varphi \circ w$ by w. From now on we set $\pi \coloneqq w \circ j_1\colon X_1(N) \to E$, where j_1 is the natural map $X_1(N) \to J_1(N) \to A_f$. The pullback $\pi^*(\omega_E)$ lies in the K-vector space spanned by the form h corresponding to β, so we have $\pi^*(\omega_E) = \gamma \cdot h$ for some $\gamma \in K^*$.

Lemma 2.5.1. We have $\dfrac{{}^{\nu}\gamma}{\gamma} = \pm 1$ and therefore $\gamma^2 = \pm N_{K/\mathbb{Q}}(\gamma)$.

Proof. Let $\omega'_E = \omega_E/\gamma$ and $\omega'_{{}^{\nu}E} = \omega_{{}^{\nu}E}/{}^{\nu}\gamma$, so that $\pi^*(\omega'_E) = h$ and ${}^{\nu}\pi^*(\omega'_{{}^{\nu}E}) = {}^{\nu}h$. As noticed in [30, p. 488], there exists an isogeny $\mu_\nu\colon E \to {}^{\nu}E$ induced by the action of some Hecke operator T_p on $J_1(N)$ for an inert prime p such that $\mu_\nu^*(\omega'_{{}^{\nu}E}) = {}^{\nu}\lambda_p \cdot \omega'_E$

where λ_p is the p-th coefficient of h. This implies $\mu_\nu^*(\omega_{{}^\nu E}) = {}^\nu\lambda_p \cdot \frac{{}^\nu\gamma}{\gamma} \cdot \omega_E$. On the other hand, $\mathrm{Hom}(E, {}^\nu E) \otimes \mathbb{Q} \simeq \mathbb{Q}$ and this means that there exists some $s \in \mathbb{Q}^*$ such that $\mu_\nu = s \cdot \mu$ and thus

$$\mu^*(\omega_{{}^\nu E}) = \frac{{}^\nu\lambda_p}{s} \cdot \frac{{}^\nu\gamma}{\gamma} \cdot \omega_E.$$

This implies that $N_{K/\mathbb{Q}}\left(\frac{{}^\nu\lambda_p}{s}\right) = m$. Now recall that $\lambda_p = \dfrac{a_p + \kappa^\sigma a_p}{1+\kappa}$. Since p is inert, the computations of section 2.4 show that a_p equals $t\sqrt{m}$ for some $t \in \mathbb{Q}$. Thus we have

$$\lambda_p = t\sqrt{m} \cdot \frac{1-\kappa}{1+\kappa},$$

which implies $t = \pm s$ because $N_{K/\mathbb{Q}}(\lambda_p) = \eta s^2 m$ and $N_{K/\mathbb{Q}}\left(\frac{1-\kappa}{1+\kappa}\right) = \eta$. But now

$$\frac{\lambda_p}{s} = \pm\sqrt{m} \cdot \frac{1 - \frac{\sqrt{\Delta_K}}{p/q+1/q\sqrt{m}}}{1 + \frac{\sqrt{\Delta_K}}{p/q+1/q\sqrt{m}}} = \pm\sqrt{m} \cdot \frac{{}^\nu\alpha + \sqrt{m}}{\alpha + \sqrt{m}} = \pm{}^\nu\alpha$$

and therefore $\dfrac{{}^\nu\lambda_p}{s} = \pm\alpha$, showing that $\dfrac{{}^\nu\gamma}{\gamma} = \pm 1$ because $\mu^*(\omega_{{}^\nu E}) = \alpha \cdot \omega_E$. □

2.5.1 The images 0 and $i\infty$ on E

The goal of this section is to prove that the points $\pi(0), \pi(i\infty) \in E(\overline{\mathbb{Q}})$ are defined over K. If Γ is a subgroup of the modular group $\mathrm{SL}_2(\mathbb{Z})$ such that $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$, then the modular curve $X(\Gamma)$ has a model over $\mathbb{Q}$; however, its cusps may not be defined over $\mathbb{Q}$. In fact the following theorem holds.

Theorem 2.5.2 (Stevens, [76])**.** Let Γ be as above. Then:

i) the cusps of $X(\Gamma)$ are defined over $\mathbb{Q}(\xi_N)$ (where $\xi_N = e^{2\pi i/N}$);

ii) for $d \in (\mathbb{Z}/N\mathbb{Z})^*$ let τ_d be the element of $\mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q})$ satisfying ${}^{\tau_d}\xi_N = \xi_N^d$ and let $\binom{x}{y}$ be a cusp of Γ. Then

$${}^{\tau_d}\binom{x}{y} = \binom{x}{d'y},$$

where d' is a multiplicative inverse of d modulo N.

Let $\pi\colon X_1(N) \to E$ be our modular parametrization, which is defined over K. Recall that π is the composition of the map $j_1\colon X_1(N) \to A_f$ and the map $w\colon A_f \to E$. The character χ can be viewed as a Dirichlet character modulo N and if $H = \ker\chi$ then $\mathbb{Q}(\xi_N)^H = K$. Let us introduce the following congruence subgroup:

$$\Gamma_H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)\colon a, d \in H \right\}.$$

Lemma 2.5.3. The points $\pi(0), \pi(i\infty) \in E(\overline{\mathbb{Q}})$ are defined over K.

Proof. First notice that $\Gamma_1(N) \subseteq \Gamma_H \subseteq \Gamma_0(N)$ and therefore we can apply Theorem 2.5.2 to $X(\Gamma_H)$. The cusp $i\infty \in X(\Gamma_H)$, which is represented by $\binom{1}{0}$ is in fact defined over $\mathbb{Q}$ since for every $d \in (\mathbb{Z}/N\mathbb{Z})^*$ one has ${}^{\tau_d}\binom{1}{0} = \binom{1}{0}$. On the other hand, ${}^{\tau_d}\binom{0}{1} = \binom{0}{d'}$. Thus if $d \in H$ also $d' \in H$ and the cusps $\binom{0}{1}$ and $\binom{0}{d'}$ are equivalent via any element of Γ_H of the form $\begin{pmatrix} a & Nb \\ Nc & d' \end{pmatrix}$ with $a, b, c \in \mathbb{Z}$. This shows that the cusp $0 \in X(\Gamma_H)$ is defined over K. Now observe that $f \in S_2(\Gamma_0(N), \varepsilon)$ and $S_2(\Gamma_0(N), \varepsilon) \subseteq S_2(\Gamma_H)$ by definition of Γ_H because either ε is trivial or $\varepsilon = \chi$. This shows that A_f is a quotient of the jacobian of $X(\Gamma_H)$. Thus the following diagram of varieties over $\mathbb{Q}$ commutes:

$$\begin{array}{ccc} X_1(N) & \xrightarrow{p} & X(\Gamma_H) \\ {\scriptstyle j_1}\downarrow & \swarrow_{j_2} & \\ A_f & & \end{array}$$

where p is the map induced by the inclusion $\Gamma_1(N) \subseteq \Gamma_H$ and j_2 is defined analogously to j_1, namely it is the composition $X(\Gamma_H) \to J(\Gamma_H) \to A_f$. Now the claim follows from the fact that $p(0) = 0$ and $p(i\infty) = i\infty$. □

We shall now distinguish the two cases $\Delta_K > 0$ and $\Delta_K < 0$.

2.5.2 K is real

First we recall the following lemma.

Lemma 2.5.4. Let $\Lambda \subseteq \mathbb{C}$ be a lattice with modular invariants $g_2(\Lambda), g_3(\Lambda) \in \mathbb{R}$. Then Λ has a $\mathbb{Z}$-basis $\{\omega_1, \omega_2\}$ with $\omega_1 \in \mathbb{R}_{>0}$ and $\Im(\omega_2) > 0$. Moreover, such ω_1 is unique.

Proof. Note that for every lattice Λ we have $\overline{g_i(\Lambda)} = g_i(\overline{\Lambda})$ for $i = 2, 3$ where the bar denotes complex conjugation. Since $g_2(\Lambda), g_3(\Lambda) \in \mathbb{R}$, this implies that $\Lambda = \overline{\Lambda}$. Therefore we can let $\omega_1 \coloneqq \min\{|\omega| \colon \omega \in \Lambda \cap \mathbb{R} \setminus \{0\}\}$ (note that this set is always nonempty). If $\{x, y\}$ is a $\mathbb{Z}$-basis for Λ, then $\omega_1 = ax + by$ for some $a, b \in \mathbb{Z}$ and (a, b) must be 1 by the minimality of ω_1. Thus $\{\omega_1\}$ can be completed to a $\mathbb{Z}$-basis of Λ and we have the claim. □

Let Λ and Λ_ν be the period lattices of (E, ω_E) and $({}^\nu E, \omega_{\nu E})$, respectively. These can be identified respectively with $\left\{\int_\gamma \omega_E \colon \gamma \in H_1(E, \mathbb{Z})\right\}$ and $\left\{\int_\gamma \omega_{\nu E} \colon \gamma \in H_1({}^\nu E, \mathbb{Z})\right\}$. Since K is real, complex conjugation acts on $E(\mathbb{C})$ and consequently induces involutions ι, ι_ν on $H_1(E, \mathbb{Z})$ and $H_1({}^\nu E, \mathbb{Z})$, respectively. Therefore it is possible to find bases $\{\gamma_1, \gamma_2\}$ of $H_1(E, \mathbb{Z})$ and $\{\gamma_{1,\nu}, \gamma_{2,\nu}\}$ of $H_1({}^\nu E, \mathbb{Z})$ such that $\iota(\gamma_1) = \gamma_1$ and $\iota_\nu(\gamma_{1,\nu}) = \gamma_{1,\nu}$. Let

$$\omega_1 \coloneqq \int_{\gamma_1} \omega_E \text{ and } \omega_{1,\nu} \coloneqq \int_{\gamma_{1,\nu}} \omega_{\nu E}.$$

Then $\omega_1, \omega_{1,\nu}$ are the unique positive real elements of Λ and Λ_ν respectively which can be completed to bases as in Lemma 2.5.4.

Definition 2.5.5. The positive real numbers ω_1 and $\omega_{1,\nu}$ are called the *real periods* of (E, ω_E).

Since we have $\alpha\Lambda \subseteq \Lambda_\nu$, there exist $a, b \in \mathbb{Z}$ such that $\alpha\omega_1 = a\omega_{1,\nu} + b\omega_{2,\nu}$. Since $\omega_1, \omega_{1,\nu}, \alpha$ are real, b must be equal to 0. Therefore the following relation holds, for some non-zero integer a:

$$\omega_{1,\nu} = \frac{\alpha}{a}\omega_1. \tag{2.16}$$

Note that a divides m because $\alpha\Lambda$ is a sublattice of Λ_ν of index m. We are now ready to compute with (2.15). Let $t \coloneqq |E(K)_{\mathrm{tors}}|$. Then we have

$$t^2 \cdot L(E/K, 1) = \tag{2.17}$$

$$= \frac{2+\kappa+\eta^\sigma\kappa}{4} \cdot \frac{1}{\gamma^2} \cdot \left(t \cdot \int_{\{0,i\infty\}} \pi^*(\omega_E) \right)^2 + \frac{2-\kappa-\eta^\sigma\kappa}{4} \cdot \frac{1}{{}^\nu\gamma^2} \cdot \left(t \cdot \int_{\{0,i\infty\}} {}^\nu\pi^*(\omega_{{}^\nu E}) \right)^2.$$

Now use the fact that $t \cdot \displaystyle\int_{\{0,i\infty\}} \pi^*(\omega_E) = \int_{t\cdot\pi_*\{0,i\infty\}} \omega_E$. Then note that $\pi_*\{0, i\infty\} \in H_1(E, \mathbb{Q})$ by Theorem 2.1.3 and so by Lemma 2.5.3 we have $\pi(0) - \pi(i\infty) \in E(K)_{\mathrm{tors}}$. This implies that $t \cdot \pi_*\{0, i\infty\} \in H_1(E, \mathbb{Z})$; moreover points on the imaginary axis in $\mathcal{H}$ are defined over $\mathbb{R}$ because complex conjugation on $X_1(N)$ corresponds to reflection with respect to the imaginary axis and the parametrization π is defined over $\mathbb{R}$ once we have chosen an embedding $K \to \mathbb{R}$. Thanks to these remarks, we can say that $t \cdot \pi_*\{0, i\infty\} \in H_1(E, \mathbb{Z})$ is invariant under complex conjugation and therefore there exists an integer M such that

$$\int_{t\cdot\pi_*\{0,i\infty\}} \omega_E = M\omega_1.$$

The above argument can be repeated analogously for ${}^\nu\pi$, implying the existence of an integer M' such that

$$\int_{t\cdot{}^\nu\pi_*\{0,i\infty\}} \omega_{{}^\nu E} = M'\omega_{1,\nu}.$$

Despite the fact that the argument used for ${}^\nu\pi$ is the same as the one used for π, the integers M and M' do not seem to be deeply related; in the example of level 229 cited in [30, p. 499] one has $M \neq 0$ while $M' = 0$ (setting $f = f_2$ and ${}^\sigma f = f_1$ in the notation of the paper). This is due to the fact that the eigenvalue of the Fricke involution W_{229} applied to f is exactly our κ, causing $\int_0^{i\infty} {}^\nu h(t)dt$, and consequently M', to vanish. On the other hand one can check that $L(f, 1) \cdot L({}^\sigma f, 1)$ is non-zero, implying that $M \neq 0$.

Finally, note that $\eta^\sigma\kappa = \dfrac{\sqrt{\Delta_K}}{{}^\sigma\beta}$ so that

$$\frac{2+\kappa+\eta^\sigma\kappa}{4} = \frac{2+\sqrt{\Delta_K}\left(\dfrac{\beta+{}^\sigma\beta}{\Delta_K}\right)}{4} = \frac{\alpha}{2q\sqrt{\Delta_K}}$$

and symmetrically

$$\frac{2-\kappa-\eta^\sigma\kappa}{4} = -\frac{{}^\nu\alpha}{2q\sqrt{\Delta_K}}.$$

Substituting everything in (2.17) and keeping (2.16) and Lemma 2.5.1 in mind we get

$$t^2 \cdot L(E/K,1) = \pm\frac{1}{2q\sqrt{\Delta_K}N(\gamma)}\left(\alpha \cdot M^2 \cdot \omega_1^2 - {}^{\nu}\alpha \cdot M' \cdot \omega_{1,\nu}^2\right) = \\ = \pm\frac{\omega_1\omega_{1,\nu}}{2q\sqrt{\Delta_K}N(\gamma)} \cdot \left(aM^2 - \frac{m}{a}M'^2\right),$$

which shows that $L(E/K,1) \cdot \dfrac{\sqrt{\Delta_K}}{\omega_1\omega_{1,\nu}} \in \mathbb{Q}$, and since $\dfrac{m}{a} \in \mathbb{Z}$ we get that

$$L(E/K,1) = \frac{\omega_1\omega_{1,\nu}}{2q|E(K)_{\text{tors}}|^2\sqrt{\Delta_K}} \cdot \frac{w}{|N(\gamma)|} \text{ for some } w \in \mathbb{Z}. \tag{2.18}$$

2.5.3 K is imaginary

The first observation in this case is that

$$\frac{(1-\kappa)(1-\eta^\sigma\kappa)}{4}L({}^{\nu}h,1)^2 = \overline{\frac{(1+\kappa)(1+\eta^\sigma\kappa)}{4}L(h,1)^2},$$

so that equation (2.15) can be read as

$$L(E/K,1) = 2\Re\left(\frac{(1+\kappa)(1+\eta^\sigma\kappa)}{4}L(h,1)^2\right).$$

The same argument with $t \coloneqq |E(K)_{\text{tors}}|$ applies as in the case $\Delta_K > 0$, so that we have $t \cdot \pi_*\{0, i\infty\} \in H_1(E,\mathbb{Z})$. Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be the period lattice of (E,ω_E). We can assume that $\omega_{{}^{\nu}E}$ is such that $\overline{\Lambda} = \mathbb{Z}\overline{\omega_1} + \mathbb{Z}\overline{\omega_2}$ is the period lattice of $({}^{\nu}E, \omega_{{}^{\nu}E})$. Thus there exist $a,b,c,d \in \mathbb{Z}$ such that

$$\begin{cases} \alpha\omega_1 = a\overline{\omega_1} + b\overline{\omega_2} \\ \alpha\omega_2 = c\overline{\omega_1} + d\overline{\omega_2}. \end{cases}$$

This time we have

$$\int_{t\cdot\pi_*\{0,i\infty\}} \omega_E = (x\omega_1 + y\omega_2)$$

for some $x,y \in \mathbb{Z}$ and thus we get

$$t^2 \cdot L(E/K,1) = \Re\left(\pm\frac{\alpha}{2q\sqrt{\Delta_K}} \cdot \frac{1}{N(\gamma)} \cdot (x\omega_1 + y\omega_2)^2\right) = \\ = \pm\frac{2}{2q\sqrt{|\Delta_K|}N(\gamma)}\Im((x\omega_1 + y\omega_2)(x(a\overline{\omega_1} + b\overline{\omega_2}) + y(c\overline{\omega_1} + d\overline{\omega_2}))) = \\ = \pm\frac{2\Im(\omega_1\overline{\omega_2})}{2q\sqrt{|\Delta_K|}N(\gamma)} \cdot (xy(a-d) + y^2c - x^2b),$$

where we used the fact that $\sqrt{\Delta_K}$ is purely imaginary. Since $xy(a-d) + y^2c - x^2b \in \mathbb{Z}$ we get $L(E/K,1) \cdot \dfrac{\sqrt{|\Delta_K|}}{2\Im(\omega_1\overline{\omega_2})} \in \mathbb{Q}$ and therefore

$$L(E/K,1) = \frac{2\Im(\omega_1\overline{\omega_2})}{2q|E(K)_{\text{tors}}|^2\sqrt{|\Delta_K|}} \cdot \frac{w}{N(\gamma)} \text{ for some } w \in \mathbb{Z}. \tag{2.19}$$

The term $\Im(\omega_1\overline{\omega_2})$ coincides (in absolute value) with the covolume of Λ.

2.6 The Manin ideal

The factor $N(\gamma)$ in (2.18) and (2.19) should play a similar role to the one played by the Manin constant c of (2.5). Let $\mathcal{E}$ be the Néron model of E over $\mathcal{O}_K$. Then $H^0(\mathcal{E}, \Omega^1_{\mathcal{E}/\mathcal{O}_K})$ is a locally free $\mathcal{O}_K$-module of rank 1 inside $H^0(E, \Omega^1_{E/K})$. In [30], the authors introduce the following fractional ideal attached to a parametrization $\pi\colon X_1(N) \to E$ over K.

Definition 2.6.1. The *Manin ideal* $\mathfrak{c}(\pi)$ attached to the parametrization π is the fractional ideal of K satisfying:

$$\pi^* H^0(\mathcal{E}, \Omega^1_{\mathcal{E}/\mathcal{O}_K}) = \mathfrak{c}(\pi) \left(\pi^* H^0(E, \Omega^1_{E/K}) \cap \mathcal{O}_K[\![q]\!] \right).$$

If $\omega \in H^0(E, \Omega^1_{E/K})$ is non-zero, let

$$\mathfrak{m}_\omega(\pi) = \{x \in K\colon x \cdot \pi^*(\omega) \in \mathcal{O}_K[\![q]\!]dq\}.$$

Following [30] again, we define the *Weierstrass ideal* attached to the pair (E, ω) as the fractional ideal of K defined by

$$\delta_\omega = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\omega/\omega_{\mathfrak{p}})},$$

where $\mathfrak{p}$ varies among all prime ideals of $\mathcal{O}_K$ and $\omega_{\mathfrak{p}}$ is a minimal differential at $\mathfrak{p}$.

Lemma 2.6.2 ([30])**.** For any non-zero $\omega \in H^0(E, \Omega^1_{E/K})$ we have

$$\mathfrak{c}(\pi) = (\mathfrak{m}_\omega(\pi)\delta_\omega)^{-1}.$$

In analogy with Theorem 2.1.1, the following holds.

Theorem 2.6.3 ([30])**.** The Manin ideal $\mathfrak{c}(\pi)$ is an integral ideal.

The set of pairs (E, π), where E is a $\mathbb{Q}$-curve completely defined over K and $\pi\colon X_1(N) \to E$ is a modular parametrization over K, can be given the same ordering we used in section 2.1 for parametrizations over $\mathbb{Q}$: given two parametrizations (E, π) and (E', π') we say that (E', π') *dominates* (E, π), and we write $(E', \pi') \geq (E, \pi)$, if there exists an isogeny $\varphi\colon E' \to E$ such that $\pi = \pi' \circ \varphi$. A maximal element with respect to this ordering is called an *optimal parametrization*, and it can be shown that every parametrization factors through an optimal one.

Conjecture 2.1.2 is therefore generalized as follows in [30].

Conjecture 2.6.4 (Generalized Manin conjecture)**.** Let $\pi\colon X_1(N) \to E$ be an optimal parametrization. Then $\mathfrak{c}(\pi) = (1)$.

2.6.1 The term $N_{K/\mathbb{Q}}(\gamma)$

Let us come back to our parametrization $\pi\colon X_1(N) \to E$ defined over K. Recall that $\pi^*(\omega_E) = \gamma \cdot h$. Now let $\pi'\colon X_1(N) \to E'$ be an optimal parametrization and $\psi\colon E' \to E$ a K-isogeny such that $\pi = \psi \circ \pi'$. Note that, as we did in section 2.1, we can assume that ψ is an isogeny of minimal degree in $\mathrm{Hom}(E', E)$. In fact, let φ be an element of minimal degree in $\mathrm{Hom}(E', E)$. Then there exists some integer k such that $\psi = k\varphi$.

Let $\overline{\pi} \coloneqq \varphi \circ \pi'$. Since $\pi = [k] \circ \overline{\pi}$, where $[k]$ denotes multiplication by k, we have $\overline{\pi}^*(\omega_E) = \frac{\gamma}{k} h$. Thus we could replace π by $[k] \circ \overline{\pi}$ in our computations which led to (2.18) and (2.19), and the only effect in these estimates would be to replace γ by γ/k, which multiplies the value of $L(E/K, 1)$ by k^2. Therefore we can assume $\psi = \varphi$. The next step is to understand how $\mathfrak{c}(\pi)$ and $\mathfrak{c}(\pi')$ are related. Note that

$$\mathfrak{m}_{\psi^*(\omega_E)}(\pi') = \{x \in K \colon x \cdot \pi'^*(\varphi^*(\omega_E)) \in \mathcal{O}_K[\![q]\!]\} = \mathfrak{m}_{\omega_E}(\pi),$$

so that

$$\mathfrak{c}(\pi) = \mathfrak{c}(\pi')\delta_{\psi^*(\omega_E)}\delta_{\omega_E}^{-1}.$$

If we set $\widetilde{\omega}_E \coloneqq \frac{1}{\gamma}\omega_E$, then we have $\pi^*(\widetilde{\omega}_E) = h$ and therefore $\mathfrak{m}_{\widetilde{\omega}_E}(\pi)$ coincides with the denominator ideal of h, i.e. the ideal

$$D_h = \{x \in K \colon x \cdot h \in \mathcal{O}_K[\![q]\!]\}.$$

Note that this is an integral ideal because h is normalized. Thus we have

$$N_{K/\mathbb{Q}}(D_h) = N_{K/\mathbb{Q}}(\mathfrak{m}_{\widetilde{\omega}_E}(\pi)) = N_{K/\mathbb{Q}}(\mathfrak{c}(\pi')^{-1}\delta_{\psi^*(\widetilde{\omega}_E)}^{-1}) = \frac{1}{N_{K/\mathbb{Q}}(\delta_{\psi^*(\widetilde{\omega}_E)})} \tag{2.20}$$

under conjecture 2.6.4. It is easy to see that

$$\delta_{\psi^*(\widetilde{\omega}_E)} = \prod_{\mathfrak{p}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\psi^*(\widetilde{\omega}_E)/\omega'_{\mathfrak{p}})} = \prod_{\mathfrak{p}} \mathfrak{p}^{-\operatorname{ord}_{\mathfrak{p}}(\gamma)} \cdot \prod_{p} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\psi^*(\omega_E)/\omega'_{\mathfrak{p}})},$$

where $\omega'_{\mathfrak{p}}$ is a minimal differential at $\mathfrak{p}$ on E', and thus

$$N_{K/\mathbb{Q}}(\delta_{\psi^*(\widetilde{\omega}_E)}) = \frac{N_{K/\mathbb{Q}}(\delta_{\psi^*(\omega_E)})}{N_{K/\mathbb{Q}}(\gamma)},$$

where $N_{K/\mathbb{Q}}(\gamma)$ is the norm of the fractional ideal generated by γ, which coincides with the absolute value of the norm of the element γ. By (2.20) we get

$$\frac{1}{N_{K/\mathbb{Q}}(\gamma)} = \frac{1}{N_{K/\mathbb{Q}}(D_h) N_{K/\mathbb{Q}}(\delta_{\psi^*(\omega_E)})}. \tag{2.21}$$

Next we claim that there exists an integer $v > 0$ such that

$$N_{K/\mathbb{Q}}(\delta_{\psi^*(\omega_E)}) \cdot v = N_{K/\mathbb{Q}}(\delta_{\omega_E}) N_{K/\mathbb{Q}}(\deg \psi). \tag{2.22}$$

Let ω' be a differential on E' and let $a, b \in K$ be such that $\psi^*(\omega_E) = a\omega'$ and $\widehat{\psi}^*(\omega') = b\omega_E$ where $\widehat{\psi}$ is the dual isogeny, so that $ab = \deg \psi$. For each prime $\mathfrak{p}$ of K let $a_{\mathfrak{p}}, b_{\mathfrak{p}} \in K$ be such that $\omega_E = a_{\mathfrak{p}}\omega_{\mathfrak{p}}$ and $\omega' = b_{\mathfrak{p}}\omega'_{\mathfrak{p}}$. With these notations we have

$$\widehat{\psi}^*(\omega'_{\mathfrak{p}}) = \frac{ba_{\mathfrak{p}}}{b_{\mathfrak{p}}}\omega_{\mathfrak{p}}.$$

By the functoriality of the Néron model, the pullback of an integral differential is integral. Thus we have

$$\operatorname{ord}_{\mathfrak{p}}\left(\frac{ba_{\mathfrak{p}}}{b_{\mathfrak{p}}}\right) \geq 0 \text{ for all } \mathfrak{p}. \tag{2.23}$$

Now

$$\delta_{\psi^*(\omega_E)} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\psi^*(\omega_E)/\omega'_{\mathfrak{p}})} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(ab_{\mathfrak{p}}\omega'_{\mathfrak{p}}/\omega'_{\mathfrak{p}}))} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(ab_{\mathfrak{p}})},$$

while

$$\delta_{\omega_E} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\omega_E/\omega_{\mathfrak{p}})} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}})}.$$

Therefore the claim (2.22) is proved if for all $\mathfrak{p}$ we have

$$\mathrm{ord}_{\mathfrak{p}}(ab_{\mathfrak{p}}) \leq \mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}}) + \mathrm{ord}_{\mathfrak{p}}(\deg \psi).$$

In fact we can rewrite this condition, using the fact that $\mathrm{ord}_{\mathfrak{p}}(a)+\mathrm{ord}_{\mathfrak{p}}(b) = \mathrm{ord}_{\mathfrak{p}}(\deg \psi)$, as

$$\mathrm{ord}_{\mathfrak{p}}(b) + \mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}}) - \mathrm{ord}_{\mathfrak{p}}(b_{\mathfrak{p}}) \geq 0,$$

which is exactly (2.23). Finally equation (2.22) together with (2.21) implies that

$$\frac{1}{N_{K/\mathbb{Q}}(\gamma)} = \frac{v}{N_{K/\mathbb{Q}}(D_h)N_{K/\mathbb{Q}}(\delta_{\omega_E})N_{K/\mathbb{Q}}(\deg \psi)} \text{ for some } v \in \mathbb{Z}_{>0}. \tag{2.24}$$

2.7 Completing the proof

The last two things we are left to understand are the norm of the denominator ideal D_h and the degree of the isogeny ψ.

2.7.1 The denominator ideal D_h

We will now compute the denominator ideal D_h, which is integral as we already noticed. Recall that

$$h = \frac{1}{1+\kappa} f + \frac{\kappa}{1+\kappa} {}^{\sigma}f,$$

where $\kappa = \dfrac{\sqrt{\Delta_K}}{\beta}$. Let $f = \displaystyle\sum_{n=1}^{+\infty} a_n q^n$ and $h = \displaystyle\sum_{n=1}^{+\infty} \lambda_n q^n$. Then for every $n \geq 1$ we have

$$\lambda_n = \frac{1}{1+\kappa} a_n + \frac{\kappa}{1+\kappa} {}^{\sigma}a_n.$$

Recall that since f is a normalized newform, the a_n's are algebraic integers, so they belong to $\mathcal{O}_F$. If $m \equiv 2, 3 \bmod 4$ then every a_n is of the form $a + b\sqrt{m}$ for some $a, b \in \mathbb{Z}$. Thus we have

$$\begin{aligned}
\lambda_n - a &= \frac{1-\kappa}{1+\kappa} \cdot b\sqrt{m} = \frac{\sqrt{\Delta_K} - {}^{\sigma}\beta}{\sqrt{\Delta_K} + {}^{\sigma}\beta} \cdot b\sqrt{m} = \frac{q\sqrt{\Delta_K} - p + \sqrt{m}}{q\sqrt{\Delta_K} + p - \sqrt{m}} \cdot b\sqrt{m} \\
&= \frac{-{}^{\nu}\alpha + \sqrt{m}}{\alpha + \sqrt{m}} \cdot b\sqrt{m} = \frac{(-{}^{\nu}\alpha + \sqrt{m})(\alpha + \sqrt{m})}{\alpha^2 - m} \cdot b\sqrt{m} \\
&= \frac{(\alpha - {}^{\nu}\alpha)\sqrt{m}}{\alpha^2 - m} \cdot b\sqrt{m} = \frac{bm}{\alpha} = b\,{}^{\nu}\alpha,
\end{aligned}$$

using the fact that $\alpha^{\nu}\alpha = m$. If $m \equiv 1 \bmod 4$ and $a_n = a + b\left(\frac{1+\sqrt{m}}{2}\right)$ for some $a, b \in \mathbb{Z}$, one sees in the same way that

$$\lambda_n = a + \frac{b}{2} + \frac{b \cdot {}^{\nu}\alpha}{2}.$$

Let $D_{\nu_\alpha} = \{x \in \mathcal{O}_K \colon x \cdot {}^{\nu}\alpha \in \mathcal{O}_K\}$ be the denominator ideal of ${}^{\nu}\alpha$, which clearly coincides with ${}^{\nu}D_\alpha$. Then what we have shown is that if $m \equiv 2, 3 \bmod 4$ then ${}^{\nu}D_\alpha \subseteq D_h$, while if $m \equiv 1 \bmod 4$ then $2 \cdot {}^{\nu}D_\alpha \subseteq D_h$. Since $N_{K/\mathbb{Q}}(D_\alpha) = N_{K/\mathbb{Q}}({}^{\nu}D_\alpha)$, this gives us the following useful lemma.

Lemma 2.7.1. Let D_h be the denominator of h. Then we have the following two cases:

$$\begin{cases} \text{if } m \equiv 2, 3 \bmod 4 & \text{then } N_{K/\mathbb{Q}}(D_h) \mid N_{K/\mathbb{Q}}(D_\alpha) \\ \text{if } m \equiv 1 \bmod 4 & \text{then } N_{K/\mathbb{Q}}(D_h) \mid 4N_{K/\mathbb{Q}}(D_\alpha). \end{cases}$$

If in particular $\alpha \in \mathcal{O}_K$, then:

$$\begin{cases} \text{if } m \equiv 2, 3 \bmod 4 & \text{then } N_{K/\mathbb{Q}}(D_h) = 1 \\ \text{if } m \equiv 1 \bmod 4 & \text{then } N_{K/\mathbb{Q}}(D_h) \in \{1, 2, 4\}. \end{cases}$$

2.7.2 The isogeny ψ

The factor $N_{K/\mathbb{Q}}(\deg \psi) = (\deg \psi)^2$ can be treated exactly in the same way as in the case of curves over $\mathbb{Q}$. Recall that ψ is an isogeny of minimal degree in $\mathrm{Hom}_K(E', E)$. Since we might not be able to find the curve E', we bound $\deg \psi$ in the following way. Let $\{E_1, \ldots, E_n\}$ be the K-isogeny class of E. For each $i = 1, \ldots, n$ let $s_i \coloneqq \min_{\varphi}\{\deg \varphi \colon \varphi \in \mathrm{Hom}_K(E_i, E)\}$ and $s \coloneqq \gcd(s_i \colon i = 1, \ldots, n)$. Then clearly $\deg \psi$ divides s. Finding the value of s can be done algorithmically as illustrated in [5]. The author provides an algorithm which allows, given an elliptic curve C over a number field K, to compute the finite set of rational primes $\{p_1, \ldots, p_r\}$ such that C admits a K-isogeny of degree p_i for every i. Repeating this procedure a finite number of times allows us to draw a graph called the *isogeny graph* whose vertices correspond to $\{E_1, \ldots, E_n\}$ and such that for $i \neq j$ there is an edge from E_i to E_j if and only if there is an isogeny of prime degree between E_i and E_j. This is a (weighted, undirected) connected graph because every isogeny can be decomposed as a chain of isogenies of prime degree.

Remark 2.7.2. Assume that E and ${}^{\nu}E$ are not isomorphic. Since being a $\mathbb{Q}$-curve is an invariant condition under isogeny and by assumption no curve in the isogeny class of E is defined over $\mathbb{Q}$, the isogeny graph of E has an even number of vertices, call them $\{E_1, \ldots, E_{2n}\}$. These can be labeled in the following way: we assume $E = E_1$ and for every $i = 1, \ldots, n$ we set $E_{n+i} = {}^{\nu}E_i$. Then in order to find s it is enough to consider the subgraph $\{E_1, \ldots, E_n\}$ because if any curve $E_{n+i} \in \{E_{n+1}, \ldots, E_{2n}\}$ admits an optimal parametrization, then so does E_i: it is enough to consider the conjugate parametrization.

2.8 The main theorem

Let us now collect all the ingredients we have in order to be able to state our result in a more compact way.

Let K be a quadratic number field of discriminant Δ_K with Galois group $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \nu\}$. Let E/K be a $\mathbb{Q}$-curve with no CM, completely defined over K and not isogenous to an elliptic curve defined over $\mathbb{Q}$. Let $\mu\colon E \to {}^{\nu}E$ be an isogeny and let m be the integer such that ${}^{\nu}\mu\mu$ coincides with multiplication by m. Let ω_E be a invariant differential on E and let $\omega_{\nu E}$ be an invariant differential on ${}^{\nu}E$ such that $\mu^*(\omega_{\nu E}) = \alpha \cdot \omega_E$, where $\alpha = p + q\sqrt{\Delta_K} \in K$ has norm m. Let $D_\alpha = \{x \in \mathcal{O}_K\colon x \cdot \alpha \in \mathcal{O}_K\}$ be the denominator ideal of α. Let δ_{ω_E} be the Weierstrass ideal of (E, ω_E).

Let $\omega_1, \omega_{1,\nu}$ be the (positive) real periods of (E, ω_E) if K is real and let $\{\omega_1, \omega_2\}$ be a basis for the period lattice of (E, ω_E) such that $\Im(\omega_1\overline{\omega_2}) > 0$ if K is imaginary. Define

$$\Omega_E \coloneqq \begin{cases} \dfrac{\omega_1 \cdot \omega_{1,\nu}}{N_{K/\mathbb{Q}}(\delta_{\omega_E})} & \text{if } K \text{ is real} \\ \dfrac{2\Im(\omega_1\overline{\omega_2})}{N_{K/\mathbb{Q}}(\delta_{\omega_E})} & \text{if } K \text{ is imaginary.} \end{cases}$$

Notice that the product formula implies that Ω_E does not depend on ω_E.

Remark 2.8.1. If ω_E is a global minimal differential on E, one has that $\delta_{\omega_E} = (1)$. This justifies the fact that in section 2.1 we omitted the term coming from δ_{ω_E} in the definition of Ω_E for elliptic curves over $\mathbb{Q}$. The two definitions are therefore consistent.

Finally, let s be the positive integer determined in section 2.7.2.

Theorem 2.8.2. Let the notation be as above and assume that $L(E/K, 1) \neq 0$. Then the following hold:

i) $L(E/K, 1) \cdot \dfrac{\sqrt{|\Delta_K|}}{\Omega_E} \in \mathbb{Q}^*$;

ii) if we assume conjecture 2.6.4, then

$$L(E/K, 1) \cdot \frac{\sqrt{|\Delta_K|}}{\Omega_E} \cdot 2q \cdot |E(K)_{\mathrm{tors}}|^2 \cdot t \cdot N_{K/\mathbb{Q}}(D_\alpha) \cdot s^2 \in \mathbb{Z},$$

where $t = 4$ if $m \equiv 1 \bmod 4$ and $t = 1$ otherwise.

Theorem 2.8.2 is the analogue of equation 2.5 that we were seeking for. It has the same type of applications of that equation: we can use it in order to compute the L-ratio $\dfrac{L(E,1)}{\Omega_E}$ whenever such value is non-zero or to prove that $L(E, 1) = 0$ if this is the case. For this second application we can, as in section 2.1, substitute s with $s' \coloneqq \max_i\{s_i\}$, in order to get a more efficient lower bound.

2.8.1 The Birch and Swinnerton-Dyer conjecture

Let us now recall the statement of the Birch and Swinnerton-Dyer conjecture for elliptic curves over number fields. For a reference on the subject, see [23] or [33]. For an elliptic curve E over a number field K, we recall that the *algebraic rank* of E is the rank of $E(K)/E(K)_{\mathrm{tors}}$ as a $\mathbb{Z}$-module, while the *analytic rank* of E is the order of vanishing of $L(E, s)$ at the point $s = 1$. The analytic rank is only defined if $L(E, s)$ has an analytic continuation to $\mathbb{C}$ (or to any neighborhood of $s = 1$), which is not known to be true in general. Therefore we will include the statement inside the conjecture.

Conjecture 2.8.3 (Weak BSD conjecture)**.** Let E be an elliptic curve over a number field K. Then:

a) $L(E,s)$ has an analytic continuation to $\mathbb{C}$;

b) the analytic rank and the algebraic rank of E coincide.

Before stating the strong form the BSD conjecture, let us recall the definition of the following invariants attached to E.

- Let $\{P_1,\dots,P_r\}$ be a $\mathbb{Z}$-basis of $E(K)/E(K)_{\mathrm{tors}}$. The *regulator* of E over K, denoted by $R(E/K)$, is defined as

$$R(E/K) = \det(\langle P_i, P_j\rangle),$$

  where $\langle , \rangle$ is the Néron–Tate pairing of E over K.

- Let $M_K = M_K^\infty \cup M_K^0$ be the set of places of K, where M_K^∞ is the set of archimedean places and M_K^0 is the set of non-archimedean places. Choose an invariant differential ω on E. For every place $v \in M_K$, the invariant differential ω gives an invariant differential ω_v on E_{K_v}, where K_v is the completion of K at v. Let dx be the Haar measure on the ring of adèles $\mathbb{A}$ such that $\int_{\mathbb{A}/K} dx = 1$ and choose a decomposition $dx = \otimes_v dx_v$, so that dx_v is a Haar measure on K_v. Finally, for every $v \in M^0(K)$ let $L_v(E,s)$ be the local L-function at v (see [33] for details).

  The *period* of E over K is defined as:

$$P(E/K) = \prod_{v\in M_K^0} \left(L_v(E,1) \cdot \int_{E(K_v)} |\omega_v| \right) \cdot \prod_{v\in M_K^\infty} \int_{E(K_v)} |\omega_v|.$$

  By [77, Lemma 54], the product defining $P(E/K)$ is finite, since almost all factors are equal to 1. The product formula shows that $P(E/K)$ is independent of ω.

- The *Tate–Shafarevich group* of E over K is defined as

$$Ш(E/K) = \ker\left(H^1(G_K, E) \xrightarrow{\mathrm{Res}} \prod_{v\in M_K} H^1(G_{K_v}, E) \right),$$

  where G_K (resp. G_{K_v}) is the absolute Galois group of K (resp. K_v) and

$$\mathrm{Res} = \prod_{v\in M_K} \left(\mathrm{Res}_v \colon H^1(G_K, E) \to H^1(G_{K_v}, E) \right).$$

Conjecture 2.8.4 (Strong BSD conjecture)**.** The weak BSD conjecture holds and moreover we have that:

c) the Tate–Shafarevich group is finite and if r is the rank of E then:

$$\frac{L^{(r)}(E,1)}{r!} = \frac{P(E/K)\cdot R(E/K)\cdot |Ш(E/K)|}{|E(K)_{\mathrm{tors}}|^2}.$$

Let us explain the relationship between $P(E/K)$ and the quantity $\Omega_E/\sqrt{|\Delta_K|}$ appearing in Theorem 2.8.2. Recall that if $v \in M_K^0$ and $\mathcal{E}$ is a minimal model of E at v, then the *Tamagawa number* of E at v is defined as $[\mathcal{E}(K_v)\colon \mathcal{E}^0(K_v)]$ where $\mathcal{E}^0(K_v)$ is the subgroup of $\mathcal{E}(K_v)$ consisting of points which reduce to nonsingular points modulo v. Note that there are only finitely many v such that $c_v \neq 1$. In [44, pp. 92-96] it is proved that if ω is an invariant differential on E then

$$P(E/K) = \prod_{v\in M_K^0} c_v \cdot \prod_{\substack{v\in M_K^\infty \\ v \text{ real}}} \int_{E(K_v)} |\omega| \cdot \prod_{\substack{v\in M_K^\infty \\ v \text{ cplx}}} 2\int_{E(K_v)} |\omega\wedge\overline{\omega}| \cdot \frac{1}{N(\delta_\omega)\cdot\sqrt{|\Delta_K|}}. \tag{2.25}$$

Let v be a real place of K and let Λ_v be the period lattice of (E_{K_v}, ω_v). By Lemma 2.5.4, Λ_v has a basis of the form $\{\omega_{1,v}, \omega_{2,v}\}$ where $\omega_{1,v} \in \mathbb{R}_{>0}$. Then the quantity $\int_{E(K_v)} |\omega|$ coincides with $[E_{K_v}(K_v)\colon E^0_{K_v}(K_v)] \cdot \omega_{1,v}$, where $E^0(K_v)$ is the connected component of E_{K_v} containing the identity. Therefore $[E_{K_v}(K_v)\colon E^0_{K_v}(K_v)]$ is 2 precisely when the whole 2-torsion subgroup of E_{K_v} is defined over K_v, and 1 otherwise.

When v is a complex place of v and Λ_v is the period lattice of (E_{K_v}, ω_v), then the term $2\int_{E(K_v)} \omega\wedge\overline{\omega}$ coincides with twice the covolume of Λ_v.

Therefore equation (2.25) gives:

$$P(E/K) = \prod_{v\in M_K^0} c_v \cdot \prod_{\substack{v\in M_K^\infty \\ v \text{ real}}} [E_{K_v}(K_v)\colon E^0_{K_v}(K_v)] \cdot \frac{\Omega_E}{\sqrt{|\Delta_K|}}.$$

Recall that part i) of Theorem 2.8.2 tells us that if $L(E/K,1) \neq 0$ then $L(E/K,1)\cdot \dfrac{\sqrt{|\Delta_K|}}{\Omega_E} \in \mathbb{Q}^*$. Therefore our result is at least consistent with the statement of BSD when E has analytic rank 0, since it shows that the "irrational part" of $L(E/K,1)$ is $\Omega_E/\sqrt{\Delta_K}$.

2.9 Examples

In order to find examples of $\mathbb{Q}$-curves, one can follow the method indicated in [27]. Let us briefly recall it. Let $N \in \mathbb{N}$ be square-free and consider the modular curve $X_0(N)$, whose k-rational points parametrize (isomorphism classes of) pairs (E,ϕ) where E is an elliptic curve over a number field k and ϕ is a degree N isogeny with cyclic kernel defined over k. For every divisor N_1 of N, there exists an involution w_{N_1} on $X_0(N)$ which is defined as follows at non-cuspidal points: if $(E,\phi) \in Y_0(N)(k)$ and $N = N_1\cdot N_2$ then ϕ factors uniquely as $\phi_2\circ\phi_1$ where ϕ_i has degree N_i. Note that by the uniqueness of the factorization, the ϕ_i's are defined over k. On the other hand, ϕ factors as $\varphi_1\circ\varphi_2$ with φ_i of degree N_i. If $\widehat{\phi_1}$ denotes the dual isogeny of ϕ_1 then $\varphi_2\circ\widehat{\phi_1}$ is a cyclic k-rational isogeny of degree N and it therefore corresponds to a point of $Y_0(N)$ which is $w_{N_1}((E,\phi))$. The group generated by all the w_M for $M \mid N$ is an abelian group, denoted by $W(N)$, isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ where r is the number of distinct prime factors of N. The quotient of $X_0(N)$ by $W(N)$ is denoted by $X^*(N)$; given a $\mathbb{Q}$-rational point P on $X^*(N)$, its preimages on $X_0(N)$ under the quotient map $X_0(N) \to X^*(N)$ form a $G_\mathbb{Q}$-stable set whose elements correspond to $\mathbb{Q}$-curves. Conversely, in the same paper

Elkies shows that every $\mathbb{Q}$-curves is geometrically isogenous to a $\mathbb{Q}$-curve that arises in this way.

In [37], the author computes some families of $\mathbb{Q}$-curves defined over quadratic fields admitting an isogeny of small prime degree to the conjugates. Let us recall the equations of two such families (for more details see Theorem 2.2): for every square-free integer $d \neq 1$ and each rational number u let

$$E^{(2)}_{d,u}\colon y^2 = x^3 + 6(3u\sqrt{d} - 5)x - 8(9u\sqrt{d} - 7)$$

$$E^{(7)}_{d,u}\colon y^2 = x^3 - Ax + B,$$

where

$$A = 21(u^2d + 27)(15u^2d + 96u\sqrt{d} + 85)$$
$$B = 98(u^2d + 27)(27u^4d^2 + 144u^3d\sqrt{d} + 1170u^2d + 2608u\sqrt{d} + 1539).$$

Then $E^{(p)}_{d,u}$ is a $\mathbb{Q}$-curve admitting an isogeny of degree p to its conjugate. In [37, Corollary 4.3] the author explains how to construct twists of the curves in this family which are completely defined over the base field. By searching through the families above twisted by some simple values b, we used these results to construct examples of $\mathbb{Q}$-curves of positive rank completely defined over quadratic fields. As noticed in [7], the algebraic rank of such curves is necessarily even. This follows from the existence of an action of $\mathbb{Z}[\sqrt{m}]$ on $E(K)$. In particular, all curves in our examples have algebraic rank two: it can be checked using the algorithm in [72] that the rank is at most two; we will exhibit for each curve a pair of independent points of infinite order.

For every curve presented below we will compute the relevant invariants and the lower bound given by Theorem 2.8.2. Afterward, we will compute the (Galois orbit of the) newform attached to it and the corresponding sign of the functional equation. Finally, computing $L(E/K, 1)$ and $L'(E/K, 1)$ within a sufficient precision will allow us to verify the validity of the weak form of BSD conjecture for these curves. All computations have been performed using Sage [75]. The computations of $L(f, 1)$ and $L'(f, 1)$ rely on the algorithm presented in [21]. This is based on the following well-known fact (see [2] and [20]). Let $f = \sum_{n=1}^{+\infty} a_n q^n$ be a newform in $S_2(\Gamma_1(N))$. Then there exists an algebraic number $\eta_f \in \mathbb{C}^*$ of absolute value 1 such that:

$$\Lambda(f, s) = \eta_f \cdot \Lambda(f^*, 2 - s), \tag{2.26}$$

where $f^* = \sum_{n=1}^{+\infty} \overline{a_n} q^n$ and $\Lambda(f, s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(f, s)$. The number η_f is called the *sign* of the functional equation (2.26) and it is ± 1 when $\mathbb{Q}(a_n\colon n \in \mathbb{N})$ is a totally real number field. The algorithm quoted above can be also used to compute η_f, when this is not known.

Example 1

Let $d = 22$, $K = \mathbb{Q}(\sqrt{22})$, $u = -36/169$ and $b = \dfrac{91}{3} + \dfrac{13}{2}\sqrt{22}$. Then an integral model for the curve $E^{(2)}_{22,-36/169}$ twisted by b is given by

$$E\colon y^2 = x^3 - (7200684 - 1535112\sqrt{22})x + 10456553952 - 2229344208\sqrt{22}.$$

Note that since

$$j(E) = \frac{26692787554112}{2401} + \frac{5690844716544}{2401}\sqrt{22}$$

is not integral, E has no CM. There is a K-isogeny

$$\mu\colon E \to {}^{\nu}E$$

$$(x, y) \mapsto (g(x), y \cdot h(x)),$$

where

$$g(x) = \frac{(197/2 + 21\sqrt{22})x^2 - (1092 + 234\sqrt{22})x + 27378 - 5832\sqrt{22}}{x + 2184 - 468\sqrt{22}}$$

$$h(x) = \frac{-(2765/2 + 1179/4\sqrt{22})x^2 + (30732 + 6552\sqrt{22})x - 171162 - 36261\sqrt{22}}{x^2 + (4368 - 936\sqrt{22})x + 9588384 - 2044224\sqrt{22}},$$

such that ${}^{\nu}\mu\mu = -2$. Therefore $F = \mathbb{Q}(\sqrt{-2})$. If $\omega_E = \dfrac{dx}{2y}$ and $\omega_{{}^{\nu}E}$ is its conjugate, we have that $\mu^*(\omega_{{}^{\nu}E}) = (-14 + \frac{3}{2}\sqrt{88})\omega_E$, so that we can set $\alpha = -14 + \frac{3}{2}\sqrt{88}$ and consequently $\beta = -\frac{28}{3} + \frac{2}{3}\sqrt{-2}$. Clearly $N_{K/\mathbb{Q}}(\alpha) = -2$ and $N_{F/\mathbb{Q}}(\beta) = 88$. Moreover, since $\alpha \in \mathcal{O}_K$ by Lemma 2.7.1 it follows that $D_h = (1)$.

One can check that E has conductor (7). The Weierstrass ideal of the standard invariant differential is $\delta_{\omega_E} = (6)^{-1}$.

The last step is to find s as in Theorem 2.8.2. Using the algorithm described in [5], one can check that the isogeny graph of E has the following shape:

$$\begin{array}{ccc} E & \overset{2}{\text{———}} & {}^{\nu}E \\ {\scriptstyle 3}\big| & & \big|{\scriptstyle 3} \\ E_1 & \overset{2}{\text{———}} & {}^{\nu}E_1. \end{array}$$

Therefore either E possesses an optimal parametrization or E_1 does, showing that we can assume $s = 3$. The following table summarizes the invariants we need in order to apply Theorem 2.8.2.

Ω_E	q	$\lvert E(K)_{\text{tors}}\rvert$	$t \cdot N_{K/\mathbb{Q}}(D_\alpha)$	s^2
5.45882600014972	3/2	6	1	9

By Theorem 2.8.2, if $L(E/K, 1) \neq 0$ then we must have that:

$$|L(E/K, 1)| \geq \frac{5.45882600014972}{3 \cdot 36 \cdot \sqrt{88} \cdot 9} \approx 5.98675727185567 \cdot 10^{-4}.$$

Two independent points of infinite order in $E(K)$ are given by

$$P = (-1860 + 396\sqrt{22}, 75924 - 16200\sqrt{22})$$

and

$$Q = (498 - 72\sqrt{22}, -47628 + 10584\sqrt{22}).$$

The newform $f = \sum_{n=1}^{+\infty} a_n q^n$ attached to E has level $7 \cdot 88 = 616$. This implies $f \in S_2(\Gamma_1(616), \varepsilon)$, where ε is the unique primitive quadratic character such that $\overline{\mathbb{Q}}^{\ker \varepsilon} = \mathbb{Q}(\sqrt{22})$. Computing the first few terms of f, we get:

$$\begin{aligned} f = q + \sqrt{-2}q^2 - 2q^3 - 2q^4 + 2\sqrt{-2}q^5 - 2\sqrt{-2}q^6 + q^7 - \\ - 2\sqrt{-2}q^8 + q^9 - 4q^{10} + (\sqrt{-2} - 3)q^{11} + 4q^{12} - 4q^{13} + \sqrt{-2}q^{14} - \\ - 4\sqrt{-2}q^{15} + 4q^{16} + 2\sqrt{-2}q^{17} + \sqrt{-2}q^{18} - 4\sqrt{-2}q^{20} + O(q^{21}). \end{aligned}$$

Using the q-expansion above it is easy to see that $a_{616}(f) = 4 + 6\sqrt{-2}$, so that by [2, Theorem 2.1] we get that $\eta_f = \dfrac{\sqrt{88}}{4 + 6\sqrt{-2}}$.

Example 2

Let $u = -3/4$, $d = -6$, so that $K = \mathbb{Q}(\sqrt{-6})$, and $b = \dfrac{12}{7} + \dfrac{2}{7}\sqrt{-6}$. Then a global integral model for the curve $E^{(7)}_{-6,-3/4}$ twisted by b is

$$E\colon y^2 = x^3 - (4027482 - 1132380\sqrt{-6})x + 2581493976 - 1335076020\sqrt{-6},$$

which has j-invariant

$$j(E) = -\frac{12097712691}{78125} + \frac{10861109532}{78125}\sqrt{-6} \notin \mathcal{O}_K.$$

There is an isogeny $\mu\colon E \to {}^{\nu}E$ of degree 7, whose composition with ${}^{\nu}\mu$ coincides with multiplication by 7. Setting $\omega_E = \dfrac{dx}{2y}$ we obtain that $\mu^*(\omega_{{}^{\nu}E}) = (-1 + \sqrt{-6})\omega_E$ so $\alpha = -1 + \frac{1}{2}\sqrt{-24}$ and $\beta = -2 + 2\sqrt{7}$. By Lemma 2.7.1, $D_h = (1)$. The conductor of E is given by

$$\mathcal{N}(E) = (480) = (2)^5(3)(5) = (2, \sqrt{-6})^{10}(3, \sqrt{-6})^2(5, 2 + \sqrt{-6})(5, 3 + \sqrt{-6}).$$

The Weierstrass ideal attached to the standard invariant differential is

$$\delta_{\omega_E} = \left(\frac{1}{21} + \frac{1}{21}\sqrt{-6}\right)$$

and has norm $1/63$. The isogeny graph of E is given by:

$$\begin{array}{ccc} E & \overset{7}{\text{———}} & {}^{\nu}E \\ {\scriptstyle 2}\Big| & & \Big|{\scriptstyle 2} \\ E_1 & \overset{7}{\text{———}} & {}^{\nu}E_1. \end{array}$$

Ω_E	q	$\lvert E(K)_{\text{tors}}\rvert$	$t \cdot N_{K/\mathbb{Q}}(D_\alpha)$	s^2
0.663037499513841	1/2	2	1	4

Theorem 2.8.2 shows that if $L(E/K,1) \neq 0$ then:

$$|L(E/K,1)| \geq \frac{0.663037499513841}{4 \cdot \sqrt{24} \cdot 4} \approx 8.45887267706248 \cdot 10^{-3}.$$

The points

$$P = \left(\frac{29502}{25} - \frac{3546}{25}\sqrt{-6}, -\frac{391554}{125} + \frac{59292}{125}\sqrt{-6} \right)$$

and

$$Q = \left(-1674 - 1287\sqrt{-6} : -252288 - 7776\sqrt{-6}\right)$$

in $E(K)$ are independent and they have infinite order.

The newform $f = \sum_{n=1}^{+\infty} a_n q^n$ attached to E has level $480 \cdot 24 = 11520$ and since $F = \mathbb{Q}(a_n \colon n \in \mathbb{N}) = \mathbb{Q}(\sqrt{7})$, the character of f is trivial, so $f \in S_2(\Gamma_0(11520))$. The first coefficients of the q-expansion of f are:

$$f = q + q^5 + 2q^7 - 2q^{11} + 2\sqrt{7}q^{19} + O(q^{21}).$$

The sign η_f of the functional equation for f is -1.

Example 3

Let $d = 34$, $u = 7/4$, $b = 17/2 + 3/2\sqrt{34}$. An integral model for $E^{(2)}_{34,7/4}$ twisted by b is given by:

$$E \colon y^2 = x^3 + (365568 + 62730\sqrt{34})x - 111410656 - 19106640\sqrt{34}$$

and the j-invariant is

$$j(E) = \frac{1353090752}{680625} - \frac{123420416}{680625}\sqrt{34},$$

so that E has no CM. There is an isogeny $\mu \colon E \to {}^{\nu}E$ of degree 2 given by $(x,y) \mapsto (g(x), y \cdot h(x))$ as follows:

$$g(x) = \frac{(35/2 - 3\sqrt{34})x^2 + (68 - 12\sqrt{34})x + 612 + 1071\sqrt{34}}{x - 136 - 24\sqrt{34}}$$

$$h(x) = \frac{-(207/2 + 71/4\sqrt{34})x^2 - (816 + 140\sqrt{34})x - 18003 - 3179\sqrt{34}}{x^2 - (272 - 48\sqrt{34})x + 38080 - 6528\sqrt{34}}$$

and ${}^{\nu}\mu\mu$ coincides with multiplication by 2, so $F = \mathbb{Q}(\sqrt{2})$. Using $\omega_E = \dfrac{dx}{2y}$ we get $\alpha = -6 - \dfrac{1}{2}\sqrt{136}$ and $\beta = 12 - 2\sqrt{2}$. The conductor of E is

$$\mathcal{N}(E) = (1077120) = (2)^7(3)^2(5)(11)(17) = (6 - \sqrt{34})^{14}(3, 1 + \sqrt{34})^2(3, 2 + \sqrt{34})^2 \cdot$$
$$\cdot(5, 2 + \sqrt{34})(5, 3 + \sqrt{34})(11, 10 + \sqrt{34})(11, 1 + \sqrt{34})(17 - 3\sqrt{34})^2.$$

One can check that the given Weierstrass equation is a global minimal model for E, so that $\delta_{\omega_E} = (1)$. Also, the isogeny graph of E is

$$E \overset{2}{\text{---}} {}^{\nu}E,$$

so that conjecturally E possesses an optimal parametrization; therefore we can set $s = 1$.

Ω_E	q	$\lvert E(K)_{\mathrm{tors}}\rvert$	$t \cdot N_{K/\mathbb{Q}}(D_\alpha)$	s^2
0.0704074944313492	$-1/2$	2	1	1

The lower bound given by Theorem 2.8.2 is:

$$|L(E/K,1)| \geq \frac{0.0704074944313492}{4 \cdot \sqrt{136}} \approx 1.50934820976064 \cdot 10^{-3}.$$

Two independent points of infinite order in $E(K)$ are given by:

$$P = (1768 + 300\sqrt{34}, 107100 + 18360\sqrt{34})$$

and

$$Q = \left(\frac{867}{4} + \frac{65}{2}\sqrt{34}, -\frac{48025}{8} - \frac{8075}{8}\sqrt{34}\right).$$

The newform $f = \sum_{n=1}^{+\infty} a_n q^n$ attached to E has level $1077120 \cdot 136 = 146488320$ and since $F = \mathbb{Q}(a_n \colon n \in \mathbb{N}) = \mathbb{Q}(\sqrt{2})$, the character of f is trivial, so $f \in S_2(\Gamma_0(146488320))$. Its q-expansion is:

$$f = q + q^5 - q^{11} + 4\sqrt{2}q^{13} + 5\sqrt{2}q^{19} + O(q^{21}),$$

and the sign of the functional equation is again -1.

The next example, borrowed from [28, Proposition 10], exhibits a curve of algebraic rank 2 whose field of definition K coincides with the field F generated by the Fourier coefficients of the attached newform.

Example 4

Let $K = \mathbb{Q}(\sqrt{2})$ and $E \colon y^2 = x^3 + (8+8\sqrt{2})x^2 + (16+10\sqrt{2})x$. The j-invariant of E is $\frac{698048}{49} + \frac{379136}{49}\sqrt{2}$. An isogeny $\mu \colon E \to {}^{\nu}E$ of degree 2 is given by $(x,y) \mapsto (g(x), y \cdot h(x))$, where

$$g(x) = \frac{(3/2 - \sqrt{2})x^2 - (4 - 4\sqrt{2})x + 4 - \sqrt{2}}{x}$$

$$h(x) = \frac{(-5/2 + 7/4\sqrt{2})x^2 + 5 - 3\sqrt{2}}{x^2}.$$

The isogeny ${}^{\nu}\mu\mu$ coincides with multiplication by 2, so $F = K = \mathbb{Q}(\sqrt{2})$. The standard invariant differential $\omega_E = \frac{dx}{2y}$ gives us $\alpha = -2 - \frac{1}{2}\sqrt{8}$ and $\beta = 4 + 2\sqrt{2}$. The conductor of E is

$$\mathcal{N}(E) = (896) = (2)^7(7) = (\sqrt{2})^{14}(1 - 2\sqrt{2})(1 + 2\sqrt{2}).$$

The isogeny graph of E is given by

$$E \overset{2}{\text{———}} {}^{\nu}E\,.$$

The given Weierstrass equation is a global minimal model for E.

Ω_E	q	$\lvert E(K)_{\mathrm{tors}}\rvert$	$t \cdot N_{K/\mathbb{Q}}(D_\alpha)$	s^2
2.60444072643674	$-1/2$	2	1	1

The lower bound given by Theorem 2.8.2 is:

$$|L(E/K,1)| \geq \frac{2.60444072643674}{4 \cdot 8} \approx 8.13887727011480 \cdot 10^{-2}.$$

Two independent points of finite order in $E(K)$ are

$$P = (-2\sqrt{2}, -4 - 2\sqrt{2}) \text{ and } Q = (1 - 2\sqrt{2}, 1 - 2\sqrt{2}).$$

The newform $f = \sum_{n=1}^{+\infty} a_n q^n$ attached to E has level $896 \cdot 8 = 7168$ and has trivial character, so $f \in S_2(\Gamma_0(7168))$. The first terms of its q-expansion are:

$$f = q - \sqrt{2}q^3 - 2\sqrt{2}q^5 - q^7 - q^9 - 4\sqrt{2}q^{11} + 4\sqrt{2}q^{13} + 4q^{15} - 2q^{17} + \sqrt{2}q^{19} + O(q^{21}),$$

and the sign of the functional equation is -1.

We used T. Dokchitser's script "computeL", (see [22]), implemented in Sage, to check that for every newform f computed above, at least the first 14 significant digits of $L(f,1)$ and of $L({}^{\sigma}f,1)$ are equal to 0, while $L'(f,1), L'({}^{\sigma}f,1) \neq 0$. Since $L(E/K,s) = L(f,s) \cdot L({}^{\sigma}f,s)$, this proves that $L(E/K,1) = L'(E/K,1) = 0$, while $L''(E/K,1) \neq 0$. Therefore all curves in the above examples have analytic rank 2.

A rigorous analysis of the error in floating-point computations, even if possible in principle, is beyond the goal of the present work. However, we repeated the computations several times using different high precisions, and it is very unlikely that the floating-point error has any significant influence on the outcome.

We conclude with one last example of a $\mathbb{Q}$-curve E, coming from the Hecke involution on $X_1(13)$, such that $m = -1$. This means that E is isomorphic to ${}^{\nu}E$ and therefore both curves are isomorphic over $\overline{\mathbb{Q}}$ to an elliptic curve defined over $\mathbb{Q}$, but no isomorphism $E \to {}^{\nu}E$ descends to $\mathbb{Q}$. Using for example the algorithm described in [72], it is possible to check that the curve given in this example has algebraic rank 0, and we will use our main theorem to compute its L-ratio.

Example 5

Let a be a root of the polynomial $x^2 + x - 4$ and let $K := \mathbb{Q}(a) = \mathbb{Q}(\sqrt{17})$. Then the elliptic curve

$$y^2 + (1373 + 536a)xy + (482701840 + 188441104a)y = x^3 + (244408 + 95414a)x^2$$

is a $\mathbb{Q}$-curve with j-invariant $-\dfrac{60698457}{40960}$. There is an isomorphism $\mu\colon E \to {}^{\nu}E$ given by $(x,y) \mapsto (g(x,y), h(x,y))$, where

$$\begin{aligned} g(x,y) &= (473754361 - 303386704a)x - 214320 + 137248a \\ h(x,y) &= (-587942141286 + 376511211445a)x \\ &\quad - (16755744253243 - 10730180955650a)y \\ &\quad + 100734048 - 64508896a. \end{aligned}$$

Using $\omega_E = \dfrac{dx}{2y + (1373 + 536a)y + 482701840 + 188441104a}$, we get $\alpha = 17684 + 4289\sqrt{17}$, which gives immediately $D_h = (1)$. The conductor of E is given by

$$\mathcal{N}(E) = (10) = (1 - a)(2 + a)(5).$$

Note that E has non-split multiplicative reduction at 5, which is an inert prime in K. The isogeny graph of E is simply

$$\begin{array}{ccc} E & \overset{\sim}{\text{———}} & {}^{\nu}E \\ {\scriptstyle 13}\Big| & & \Big|{\scriptstyle 13} \\ E' & \overset{\sim}{\text{———}} & {}^{\nu}E'. \end{array}$$

The given Weierstrass equation for E is a global minimal model.

Here we have the table of the invariants of E used in Theorem 2.8.2:

Ω_E	q	$\lvert E(K)_{\text{tors}}\rvert$	$t \cdot N_{K/\mathbb{Q}}(D_\alpha)$	s^2
11.1808314690274	4289	13	1	169

By Lemma 2.1.4, in order to compute the L-ratio of E, i.e. the value $L(E,1)\cdot\dfrac{\sqrt{17}}{\Omega_E} \in \mathbb{Q}^*$, we only need a bound on the denominator of such number. By Theorem 2.8.2, this is given by:

$$B = 2 \cdot 4289 \cdot 169 \cdot 169 = 244996258.$$

The L-ratio for E is given by:

$$L(E,1) \cdot \frac{\sqrt{17}}{\Omega_E} = 1.$$

Since the Tamagawa numbers of E at the prime ideals $(1-a), (2+a)$ and (5) are respectively $13, 13$ and 1, the strong BSD conjecture would imply that

$$L(E,1) \cdot \frac{\sqrt{17}}{\Omega_E} = |Ш(E/K)| = 1.$$

It is possible to check using the algorithm given in [72] that $Ш(E/K)[2]$ is trivial.

The newform f attached to E belongs to $S_2(\Gamma_1(170), \varepsilon)$, for ε the unique primitive quadratic character such that $\overline{\mathbb{Q}}^{\ker\varepsilon} = K$.

$$\begin{aligned} f = q + q^2 + 3iq^3 + q^4 + iq^5 + 3iq^6 - 4iq^7 + q^8 - 6q^9 + iq^{10} + 2iq^{11} + 3iq^{12} \\ + q^{13} - 4iq^{14} - 3q^{15} + q^{16} - (4+i)q^{17} - 6q^{18} + 7q^{19} + iq^{20} + O(q^{21}). \end{aligned}$$

Using [2, Theorem 2.1] we get that the sign of the functional equation for f is $\eta_f = \dfrac{\sqrt{17}}{1+4i}$. It is possible to check numerically that $L(E,1) \neq 0$.

Chapter 3

Strongly modular twists of $\mathbb{Q}$-curves

As we saw in the previous chapter, if K is a quadratic field and E is a $\mathbb{Q}$-curve completely defined over K, then E is strongly modular. However, this is not true anymore if E is not completely defined over K.

The problem we will study in this chapter is the following: suppose we have a $\mathbb{Q}$-curve E over a number field K. Are there strongly modular curves which are $\overline{\mathbb{Q}}$-isomorphic to E?

In the first part of the chapter, we will restrict to quadratic $\mathbb{Q}$-curves. If L is the minimal field of complete definition for E (cf. Definition 3.3.3), we will find necessary and sufficient conditions, depending only on L, for the existence of strongly modular quadratic twists of E_L. As a corollary, we will obtain necessary and sufficient conditions for the existence of strongly modular twists of E.

In the last section, we will characterize completely the class of $\mathbb{Q}$-curves which are $\overline{\mathbb{Q}}$-isomorphic to a strongly modular one.

3.1 Some useful result from group cohomology

Let us start by recalling some standard facts about group cohomology that we will use. All profinite groups that we mention are endowed with their profinite topology; in particular, finite groups are discrete.

Let G be a profinite group and let A be a commutative G-module. For a complete treatment of cohomology of profinite groups, see for example [56] or [65]. Let $N \leq G$ be a normal closed subgroup. Recall that the inclusion $N \subseteq G$ induces a map for every $i \geq 1$, called *restriction*, given by

$$\mathrm{Res}\colon H^i(G, A) \to H^i(N, A).$$

On the other hand, the canonical projection $G \to G/N$ induces a map for every $i \geq 1$, called *inflation*, given by

$$\mathrm{Inf}\colon H^i(G/N, A^N) \to H^i(G, A).$$

Let $A^N \coloneqq \{a \in A \text{ s.t. } \forall\, \sigma \in N\colon {}^{\sigma}a = a\}$.

The group $H^1(N, A)$ is endowed with an action of G/N defined in the following way: for $g \in G$ and $[c] \in H^1(N, A)$ we let ${}^{g}[c]$ be the cohomology class represented by

the cocycle $h \mapsto {}^{g}c(g^{-1}hg)$ for all $h \in N$. It is easy to check that N acts as the identity, so that the action factors through the quotient.

Theorem 3.1.1. There is a natural map, called the *transgression map*

$$\mathrm{trg}\colon H^1(N,A)^{G/N} \to H^2(G/N, A^N)$$

fitting into the following exact sequence:

$$0 \longrightarrow H^1(G/N, A^N) \xrightarrow{\mathrm{Inf}} H^1(G,A) \xrightarrow{\mathrm{Res}} H^1(N,A)^{G/N} \xrightarrow{\mathrm{trg}}$$

$$\xrightarrow{\mathrm{trg}} H^2(G/N, A^N) \xrightarrow{\mathrm{Inf}} H^2(G,A).$$

Proof. We only give the construction of the map trg. A complete proof can be found for example in [56, Proposition I.1.6.5].

It is a standard fact from the theory of profinite groups that one can find a continuous section $\widetilde{\cdot}\colon G/N \to G$ of the projection $G \to G/N$ such that $\widetilde{1} = 1$. Let $[x] \in H^1(N,A)^{G/N}$ and let $\gamma \in N$. Since x is G/N-invariant, the cocycle $h \mapsto {}^{\widetilde{\gamma}}x(\widetilde{\gamma}^{-1}h\widetilde{\gamma}) - x(h)$ is a coboundary in $Z^1(N,A)$, so there is some element $y(\widetilde{\gamma}) \in A$ such that

$${}^{\widetilde{\gamma}}x(\widetilde{\gamma}^{-1}h\widetilde{\gamma}) - x(h) = {}^{h}y(\widetilde{\gamma}) - y(\widetilde{\gamma}).$$

One can show that it is possible to choose $y(\widetilde{\gamma})$ in such a way that the map $\gamma \mapsto y(\widetilde{\gamma})$ is continuous. Now for an arbitrary $\sigma = \widetilde{\gamma}h \in G$ we set $y(\sigma) = y(\widetilde{\gamma}) + {}^{\widetilde{\gamma}}x(h)$. This way we constructed a cochain $y\colon G \to A$ and the map trg is defined as $\mathrm{trg}([x]) \coloneqq [\partial(y)]$, where $\partial\colon C^1(G,A) \to C^2(G,A)$ is the usual coboundary map. One can show that $\partial(y)$ takes values in A^N and $\partial(y)(\sigma_1,\sigma_2)$ depends only on the classes of σ_1, σ_2 modulo N. □

Remark 3.1.2. Assume now that N is abelian and the action of N on A is trivial. If N is seen as a G-module via the action $(g,h) \mapsto ghg^{-1}$ for $g \in G$ and $h \in N$, then it is clear that $H^1(N,A)^{G/N} = \mathrm{Hom}(N,A)^{G/N} = \mathrm{Hom}_G(N,A)$. We want to give a more explicit description of the transgression map in this setting. Let $[x] \in H^1(N,A)$; since the action of N on A is trivial, we are free to make any choice for the map $\gamma \mapsto y(\widetilde{\gamma})$, with the notation used in the proof of the above theorem. Thus we can choose $y(\widetilde{\gamma}) = 0$ for all γ, which is obviously continuous. Therefore for $\sigma = \widetilde{\gamma}h \in G$ one has $y(\sigma) = {}^{\widetilde{\gamma}}x(h)$. For $\sigma_1, \sigma_2 \in G$ such that $\sigma_1 = \widetilde{\gamma_1}h_1$, $\sigma_2 = \widetilde{\gamma_2}h_2$ for some $\gamma_1, \gamma_2, h_1, h_2 \in N$ we have that $\sigma_1\sigma_2 = \widetilde{\gamma_1}\widetilde{\gamma_2}{}^{\widetilde{\gamma_2}^{-1}}h_1h_2$. Note that $\widetilde{\gamma_1}\widetilde{\gamma_2}\widetilde{\gamma_1\gamma_2}^{-1} \in N$ so that there is some $h \in N$ with $\widetilde{\gamma_1}\widetilde{\gamma_2} = \widetilde{\gamma_1\gamma_2}h$. Then $\sigma_1\sigma_2 = \widetilde{\gamma_1\gamma_2}h^{\widetilde{\gamma_2}^{-1}}h_1h_2$ and

$$\partial y(\sigma_1,\sigma_2) = y(\sigma_1) + {}^{\sigma_1}y(\sigma_2) - y(\sigma_1\sigma_2) = {}^{\widetilde{\gamma_1}}x(h_1) + {}^{\widetilde{\gamma_1}h\widetilde{\gamma_2}}x(h_2) - {}^{\widetilde{\gamma_1\gamma_2}}x(h^{\widetilde{\gamma_2}^{-1}}h_1h_2) =$$

$$= x({}^{\widetilde{\gamma_1}}h_1) + x({}^{\widetilde{\gamma_1}\widetilde{\gamma_2}}h_2) - x({}^{\widetilde{\gamma_1\gamma_2}}h) - x({}^{\widetilde{\gamma_1}}h_1) - x({}^{\widetilde{\gamma_1}\widetilde{\gamma_2}}h_2) = -x({}^{\widetilde{\gamma_1}\widetilde{\gamma_2}}h) =$$

$$= -x(\widetilde{\gamma_1}\widetilde{\gamma_2}\widetilde{\gamma_1\gamma_2}^{-1}),$$

where we repeatedly used the fact that $H^1(N,A)^{G/N} = \mathrm{Hom}_G(N,A)$.

Now assume that at least one of G and A is finite. This is to avoid topological issues; it is not strictly necessary but it suffices for our purposes. Let $E(G,A)$ be the set of all exact sequences of topological groups (i.e. of profinite groups if A is finite and of discrete

groups if G is finite) of the form $0 \to A \to B \xrightarrow{\pi} G \to 1$ such that the action of G on A is given by ${}^{\sigma}a = \widetilde{\sigma} a \widetilde{\sigma}^{-1}$ for some section $\widetilde{\cdot}$ of π. Define the following equivalence relation on $E(G, A)$: two exact sequences are equivalent iff there is a isomorphism $\alpha\colon B \to B'$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \alpha} & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & B' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

Let $\mathcal{E}\mathcal{X}\mathcal{T}^1(G, A)$ be the quotient set of $E(G, A)$ by this equivalence relation. This can be endowed with a commutative group structure with identity element the isomorphism class of the exact sequence $0 \to A \to A \rtimes G \to G \to 1$.

Lemma 3.1.3. There exists an isomorphism of abelian groups

$$\mathcal{E}\mathcal{X}\mathcal{T}^1(G, A) \to H^2(G, A).$$

Proof. We will only show the construction of the bijection, without proving all details. A complete proof can be found in [56, Theorem I.1.2.5].

Let $0 \to A \to B \to G \to 1$ be an element of $E(G, A)$. Conjugation of elements of A by elements of B factors through the quotient B/A because of the commutativity of A, so it gives to A a structure of G-module. Now choose a continuous section $\widetilde{\cdot}\colon G \to B$ such that $\widetilde{1} = 1$. One checks that the map $G \times G \to A$ given by $(\sigma_1, \sigma_2) \mapsto \widetilde{\sigma_1} \cdot \widetilde{\sigma_2} \cdot \widetilde{\sigma_1 \sigma_2}^{-1}$ is a continuous 2-cocycle. Further calculations show that its cohomology class does not depend on the choice of $\widetilde{\cdot}$ and that such cohomology class is trivial precisely when there exists some $\widetilde{\cdot}$ which is also a homomorphism, i.e. when B is a semidirect product of A and G.

Conversely, let $c \in Z^2(G, A)$ and equip $B \coloneqq A \times G$ with the product topology and with the following continuous multiplication:

$$(a_1, \sigma_1)(a_2, \sigma_2) \coloneqq (a_1 + {}^{\sigma_1}a_2 + c(\sigma_1, \sigma_2), \sigma_1 \sigma_2).$$

This operation turns B into a group. The identity element is $(0, 1)$ and we have

$$(a, \sigma)^{-1} = (-{}^{\sigma^{-1}}a - {}^{\sigma^{-1}}c(\sigma, \sigma^{-1}), \sigma^{-1}).$$

One then proves that the isomorphism classes of the exact sequence $0 \to A \to B \to G \to 1$ doesn't depend on the cohomology class of c. □

Corollary 3.1.4. If G acts trivially on A, there is an isomorphism of abelian groups

$$\mathcal{E}\mathcal{X}\mathcal{T}^1_c(G, A) \to H^2(G, A),$$

where $\mathcal{E}\mathcal{X}\mathcal{T}^1_c(G, A)$ is the set of isomorphism classes of central extensions of G by A.

Proof. Just note that if $0 \to A \to B \to G \to 1$ is a central extension, then B acts trivially by conjugation on A and so G acts trivially on A. Conversely, the proof of Lemma 3.1.3 shows that if the action of G on A is trivial, then conjugation makes B act trivially on A, so that the extension is central. □

From now on, we will assume that G is also abelian and that the action of G on A is trivial.

Definition 3.1.5. We say that $c \in Z^2(G, A)$ is a *symmetric cocycle* if $c(\sigma, \tau) = c(\tau, \sigma)$ for all $\sigma, \tau \in G$.

Note c is symmetric if and only if every cocycle cohomologous to c is symmetric, because coboundaries are symmetric by the commutativity of G. Moreover, the product of two symmetric cocycles is clearly a symmetric cocycle. Thus the cohomology classes in $H^2(G, A)$ represented by a symmetric cocycle form a subgroup of $H^2(G, A)$, which we denote by $H^2_s(G, A)$.

Corollary 3.1.6. The isomorphism of Lemma 3.1.3 restricts to an isomorphism

$$\mathrm{Ext}^1(G, A) \to H^2_s(G, A),$$

where $\mathrm{Ext}^1(G, A) \subseteq \mathcal{E}\mathcal{X}\mathcal{T}^1_c(G, A)$ is the subgroup of extensions $0 \to A \to B \to G \to 1$ with B abelian.

Proof. It is clear by the proof of Lemma 3.1.3 that a cocycle is symmetric if and only if in the associated group extension $0 \to A \to B \to G \to 1$ the group B is abelian. □

Lemma 3.1.7. Let A, B be abelian groups with B finite and let p be a prime such that $pB = 0$. Then

$$\mathrm{Ext}^1(B, A) \simeq \mathrm{Hom}(B, A/pA).$$

Proof. Since B is a finite dimensional $\mathbb{F}_p$-vector space, $B = (\mathbb{Z}/p\mathbb{Z})^r$ for some $r \in \mathbb{N}$. It's enough to prove the claim for $r = 1$ because $\mathrm{Hom}(B_1 \times B_2, A) \simeq \mathrm{Hom}(B_1, A) \times \mathrm{Hom}(B_2, A)$ and $\mathrm{Ext}^1(B_1 \times B_2, A) \simeq \mathrm{Ext}^1(B_1, A) \times \mathrm{Ext}^1(B_2, A)$ for all finite abelian groups A, B_1, B_2 (see for example [78]). Consider the exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{p} \mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0.$$

Taking the long exact sequence in cohomology and noting that $\mathrm{Ext}^1(\mathbb{Z}, A) = 0$ since $\mathbb{Z}$ is a projective $\mathbb{Z}$-module, we get the exact sequence

$$\mathrm{Hom}(\mathbb{Z}, A) \xrightarrow{p^*} \mathrm{Hom}(\mathbb{Z}, A) \longrightarrow \mathrm{Ext}^1(\mathbb{Z}/p\mathbb{Z}, A) \longrightarrow 0,$$

which implies that $\mathrm{Ext}^1(\mathbb{Z}/p\mathbb{Z}, A) \simeq A/pA$ since $\mathrm{Hom}(A, \mathbb{Z}) \simeq A$ and the map p^* is just multiplication by p. Now just use that $\mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, A/pA) \simeq A/pA$ to get the claim. □

The following corollary follows easily from the lemma above.

Corollary 3.1.8. Let G be finite. Let p be a prime number such that $pG = 0$ and $pA = A$. Then

$$H^2_s(G, A) = 0.$$

Theorem 3.1.9 (Künneth formula, [38])**.** Let G_1, G_2 be profinite groups and let A be a discrete G_2-module, regarded as a $G_1 \times G_2$-module via trivial action of G_1. Then there exists a decomposition

$$H^n(G_1 \times G_2, A) \simeq \bigoplus_{p+q=n} H^p(G_1, H^q(G_2, A)),$$

which is canonical with respect to G_1 for a fixed A, but is not canonical in A.

Corollary 3.1.10. Let G be a profinite group acting trivially on a discrete G-module A. Assume $G \simeq G_1 \times G_2$ for some profinite groups G_1, G_2. Then

$$H^2(G, A) \simeq H^2(G_1, A) \oplus H^2(G_2, A) \oplus \mathrm{Hom}(G_1 \otimes G_2, A),$$

where each G_i acts trivially on A.

3.2 Modularity and strong modularity

Let E be a $\mathbb{Q}$-curve over $\overline{\mathbb{Q}}$ without CM. Recall the construction of the cohomology class attached to E: for every $\sigma \in G_{\mathbb{Q}}$ choose an isogeny $\mu_\sigma \colon {}^\sigma E \to E$ in such a way that there exists a finite Galois extension $k/\mathbb{Q}$ such that $\mu_\sigma = \mu_\tau$ whenever $\sigma \equiv \tau \bmod \mathrm{Gal}(\overline{\mathbb{Q}}/k)$. Then

$$\xi(E)(\sigma, \tau) \coloneqq \mu_\sigma {}^\sigma\mu_\tau \mu_{\sigma\tau}^{-1} \in (\mathrm{End}^0_{\overline{\mathbb{Q}}}(E))^* \simeq \mathbb{Q}^*$$

defines a 2-cocycle for the trivial action of $G_{\mathbb{Q}}$ on $\mathbb{Q}^*$.

If E is completely defined over a Galois number field K, we denote by $\xi_K(E) \in Z^2(K/\mathbb{Q}, \mathbb{Q}^*)$ the 2-cocycle attached to E in the analogous way. The cohomology class of $\xi(E)$ (resp. $\xi_K(E)$) depends only on the $\overline{\mathbb{Q}}$-isogeny class (resp. K-isogeny class) of E. With a small abuse of notation, we will often talk about "the" 2-cocycle attached to E, without mentioning explicitly the system of isogenies giving rise to it.

Note that the image of $[\xi_K(E)]$ under the inflation map $H^2(K/\mathbb{Q}, \mathbb{Q}^*) \to H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$ coincides with $[\xi(E)]$.

When there is no risk of ambiguity, the cocycle $\xi(E)$ (resp. $\xi_K(E)$) will be denoted by ξ (resp. ξ_K).

Note that since $\mathbb{Q}^* \simeq \mathbb{Q}_+^* \times \{\pm 1\}$, where $\mathbb{Q}_+^*$ is the multiplicative group of positive rational numbers, the 2-cocycle ξ (resp. ξ_K) decomposes as the product of a 2-cocycle $\xi^{\deg} \in Z^2(G_{\mathbb{Q}}, \mathbb{Q}_+^*)$ and a 2-cocycle $\xi^{\pm} \in Z^2(G_{\mathbb{Q}}, \{\pm 1\})$ (and analogously for ξ_K). The decomposition of $\mathbb{Q}^*$ into $\mathbb{Q}_+^* \times \{\pm 1\}$ induces an isomorphism

$$H^2(G_{\mathbb{Q}}, \mathbb{Q}^*) \simeq H^2(G_{\mathbb{Q}}, \mathbb{Q}_+^*) \times H^2(G_{\mathbb{Q}}, \{\pm 1\})$$

which yields a decomposition of $[\xi]$ into a *degree component* $[\xi^{\deg}] \in H^2(G_{\mathbb{Q}}, \mathbb{Q}_+^*)$ and a *sign component* $[\xi^{\pm}] \in H^2(G_{\mathbb{Q}}, \{\pm 1\})$. There are of course analogous decompositions for $H^2(K/\mathbb{Q}, \mathbb{Q}^*)$ and $[\xi_K]$.

Theorem 3.2.1 ([35, Theorem 5.3])**.** Let E be an elliptic curve defined over a Galois number field K. Then E is strongly modular over K if and only if the following three conditions hold:

i) E is completely defined over K;

ii) $\mathrm{Gal}(K/\mathbb{Q})$ is abelian;

iii) the cocycle ξ_K attached to E is symmetric, i.e. $[\xi_K] \in H^2_s(\mathrm{Gal}(K/\mathbb{Q}), \mathbb{Q}^*)$.

We will prove in Proposition 3.6.4 that asking for K to be Galois is redundant, since a $\mathbb{Q}$-curve over a non-Galois number field cannot be strongly modular.

Recall that to every cocycle $c \in Z^2(G, \mathbb{Q}^*)$, for $G = \mathrm{Gal}(K/\mathbb{Q})$, one can attach a $\mathbb{Q}$-algebra $\mathbb{Q}^c[G]$ (whose isomorphism class depends only on the cohomology class of c)

defined in the following way: as a set, it is the group algebra over $\mathbb{Q}$ generated by G, but $\sigma \cdot \tau = c(\sigma,\tau)(\sigma\tau)$. Therefore condition iii) of the theorem is equivalent to asking that $\mathbb{Q}^c[G]$ is commutative.

Suppose now that E is a $\mathbb{Q}$-curve defined over a Galois number field K. It is natural to ask if in the $\overline{\mathbb{Q}}$-isomorphism class of E there are strongly modular curves completely defined over K. Notice that since E has no CM, such isomorphic curves need to be quadratic twists of E (see for example [71, Proposition X.5.4]). Thus the problem is to understand which quadratic twists of E yield strongly modular $\mathbb{Q}$-curves.

Lemma 3.2.2 ([35, Lemma 6.1])**.** Let E be a $\mathbb{Q}$-curve completely defined over a Galois number field K with attached 2-cocycle ξ_K. For $\lambda \in K^*$ let $E^{(\lambda)}$ be the twisted curve and $\xi_K^\lambda = \xi_K(E^{(\lambda)})$ be the 2-cocycle attached to the twisted curve. Then $E^{(\lambda)}$ is completely defined over K if and only if the field $K(\sqrt{\lambda})$ is Galois over $\mathbb{Q}$. In this case, the two cocycles ξ_K and ξ_K^λ differ in $H^2(K/\mathbb{Q},\mathbb{Q}^*)$ by the cohomology class in $H^2(K/\mathbb{Q},\{\pm 1\})$ attached to the exact sequence

$$1 \to \mathrm{Gal}(K(\sqrt{\lambda})/K) \simeq \{\pm 1\} \to \mathrm{Gal}(K(\sqrt{\lambda})/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \to 1. \tag{3.1}$$

In particular, twisting by λ affects only the sign component of $[\xi_K]$ and not the degree component.

This lemma shows that if E is a $\mathbb{Q}$-curve completely defined over a Galois number field K, then there exists a quadratic twist $E^{(\lambda)}$ which is strongly modular if and only if the following conditions are satisfied.

i) $K/\mathbb{Q}$ is abelian;

ii) there exists $\lambda \in K$ such that:

   a) $K(\sqrt{\lambda})$ is Galois over $\mathbb{Q}$;
   b) $[\xi_K^\lambda] \in H^2_s(K/\mathbb{Q},\mathbb{Q}^*)$.

Remark 3.2.3. Note that a cohomology class $c \in H^2(K/\mathbb{Q},\mathbb{Q}^*)$ is symmetric if and only if both its sign component and its degree component are symmetric. For $\sigma,\tau \in \mathrm{Gal}(K/\mathbb{Q})$ the fact that $\xi_K(\sigma,\tau) = \mu_\sigma{}^\sigma\mu_\tau\mu_{\sigma\tau}^{-1}$ implies that $\xi_K(\sigma,\tau)^2 = \deg(\mu_\sigma)\cdot\deg(\mu_\tau)\cdot \deg(\mu_{\sigma\tau})^{-1}$ and since $K/\mathbb{Q}$ is an abelian extension, this implies that $\xi_K(\sigma,\tau)^2 = \xi_K(\tau,\sigma)^2$, showing that the degree component of $[\xi_K]$ is always symmetric. Therefore condition b) above can be replaced by:

b′) $[\xi_K^{\lambda,\pm}] \in H^2_s(K/\mathbb{Q},\{\pm 1\})$.

3.3 The minimal field of complete definition

The goal of this section is to describe the smallest field over which a $\mathbb{Q}$-curve is completely defined. We start by recalling the following elementary lemma.

Lemma 3.3.1. Let K/F be a Galois extension of number fields with Galois group G. Let $\lambda_1,\dots,\lambda_n \in \overline{\mathbb{Q}}$ be such that $\lambda_i^2 \in K$ for all $i \in \{1,\dots,n\}$. Let $L = K(\lambda_1,\dots,\lambda_n)$. Then the normal closure L^N of L over F coincides with $M \coloneqq K({}^\sigma\lambda_i \colon i \in \{1,\dots,n\}, \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/F))$.

Proof. For every $i \in \{1, \dots, n\}$, set $k_i \coloneqq \lambda_i^2$.

First we show that $M \subseteq L^N$. It is enough to show that ${}^{\sigma}\lambda_i \in L^N$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ and all $i \in \{1, \dots, n\}$. Note that $({}^{\sigma}\lambda_i)^2 = {}^{\sigma}k_i$ and since K/F is Galois, there exists some $\overline{\sigma} \in G$ such that ${}^{\sigma}k_i = {}^{\overline{\sigma}}k_i$. Now choose $\widetilde{\sigma} \in \mathrm{Gal}(L^N/F)$ such that $\widetilde{\sigma}|_K = \overline{\sigma}$. Then $({}^{\widetilde{\sigma}}\lambda_i)^2 = {}^{\widetilde{\sigma}}k_i = {}^{\overline{\sigma}}k_i = {}^{\sigma}k_i$. This proves that ${}^{\widetilde{\sigma}}\lambda_i = \pm {}^{\sigma}\lambda_i$, and since ${}^{\widetilde{\sigma}}\lambda_i \in L^N$, the claim follows.

Next we show that M is normal over F, proving therefore the claim. Let $h\colon M \to \overline{\mathbb{Q}}$ be an embedding. Again, it is enough to show that $h({}^{\sigma}\lambda_i) \in M$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ and all $i \in \{1, \dots, n\}$. Note that $h({}^{\sigma}\lambda_i)^2 = h(k_i) = {}^{\tau}k_i$ for some $\tau \in G$ because K/F is Galois. Choose an element $\widetilde{\tau} \in \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ such that $\widetilde{\tau}|_K = \tau$. Then $({}^{\widetilde{\tau}}\lambda_i)^2 = {}^{\widetilde{\tau}}k_i = {}^{\tau}k_i$, which shows that $h({}^{\sigma}\lambda_i) = \pm {}^{\widetilde{\tau}}\lambda_i \in M$, proving the claim. □

Let E be a $\mathbb{Q}$-curve over a Galois number field K and let $G \coloneqq \mathrm{Gal}(K/\mathbb{Q})$.

Proposition 3.3.2. There exists a unique finite extension L/K, depending only on the K-isogeny class of E, with the following properties:

i) L is Galois over $\mathbb{Q}$;

ii) $\mathrm{Gal}(L/K)$ has exponent dividing 2;

iii) E is completely defined over L;

iv) if M is a number field containing K such that E is completely defined over M, then $L \subseteq M$.

Proof. We are going to exploit an argument already described in [59, p. 4], which we now explain. Let $\nu \in G$. Let $y^2 = x^3 + Ax + B$ be a Weierstrass equation for E, where $A, B \in K$ and let $Y^2 = X^3 + {}^{\nu}AX + {}^{\nu}B$ be a Weierstrass equation for ${}^{\nu}E$. Set $\omega_E = \dfrac{dx}{2y}$ and $\omega_{{}^{\nu}E} = \dfrac{dX}{2Y}$. Let $\mu_\nu\colon {}^{\nu}E \to E$ be a $\overline{\mathbb{Q}}$-isogeny. Suppose $\mu_\nu(X, Y) = (F_1(X, Y), F_2(X, Y))$ for some $F_1(X, Y), F_2(X, Y) \in \overline{\mathbb{Q}}(X, Y)$. Since for every $P \in {}^{\nu}E(\overline{\mathbb{Q}})$ one has that $\mu_\nu(-P) = -\mu_\nu(P)$, it follows that $F_1(x_0, y_0) = F_1(x_0, -y_0)$ and $F_2(x_0, y_0) = -F_2(x_0, -y_0)$ for all $(x_0, y_0) \in {}^{\nu}E(\overline{\mathbb{Q}})$. This shows that $F_1(X, Y)$ is of the form $G_1(X, Y^2)$ for some $G_1(X, Y) \in \overline{\mathbb{Q}}(X, Y)$ while $F_2(X, Y)$ is of the form $YG_2(X)$ for some $G_2(X) \in \overline{\mathbb{Q}}(X)$. Therefore we can assume that $\mu_\nu(X, Y) = (F_1(X), YF_2(X))$ for some $F_1(X), F_2(X) \in \overline{\mathbb{Q}}(X)$. Now let $\lambda \in \overline{\mathbb{Q}}^*$ be such that $\mu_\nu^*(\omega_E) = \lambda \cdot \omega_{{}^{\nu}E}$. Then $\dfrac{dF_1(X)}{2YF_2(X)} = \dfrac{F_1'(X)dX}{F_2(X)2Y} = \lambda\dfrac{dX}{2Y}$, and it follows that $F_2(X) = \dfrac{F_1'(X)}{\lambda}$. Thus we have that

$$\mu_\nu(X, Y) = \left(F(X), \frac{1}{\lambda}YF'(X)\right) \text{ for some } F(X) \in \overline{\mathbb{Q}}(X),\ \lambda \in \overline{\mathbb{Q}}.$$

For every $\sigma \in G_K$, the isogeny ${}^{\sigma}\mu_\nu\colon {}^{\nu}E \to E$ has the same degree as μ_ν and since E has no CM, the two isogenies have to coincide up to sign. Therefore

$${}^{\sigma}\mu_\nu(X, Y) = \left({}^{\sigma}F(X), \frac{1}{{}^{\sigma}\lambda}Y{}^{\sigma}F'(X)\right) = \left(F(X), \pm\frac{1}{\lambda}YF'(X)\right) = \pm\mu_\nu(X, Y)$$

Hence, $F(X) \in K(X)$, the isogeny μ_ν is defined over $K(\lambda)$ and $\lambda^2 \in K^*$ since for every $\sigma \in G_K$ we have that ${}^{\sigma}(\lambda^2) = \lambda^2$.

The discussion above shows that, given any collection of isogenies $\{\mu_\nu\}_{\nu\in G}$, it is possible to construct a map $\mu_\nu \mapsto \lambda_\nu \in \overline{\mathbb{Q}}^*$ where $\lambda_\nu^2 \in K$ for every $\nu \in G$. Now for every $\nu \in G$, let $\mu_\nu \in \mathrm{Hom}_{\overline{\mathbb{Q}}}({}^\nu E, E)$ be an isogeny of minimal degree. This way we determine, for all ν, some λ_ν as above. Note that choosing the other $\mathbb{Z}$-generator of $\mathrm{Hom}_{\overline{\mathbb{Q}}}({}^\nu E, E)$ corresponds to changing the sign of λ_ν. Now let $L_\nu := K(\lambda_\nu)$ and let $L := K(\lambda_\nu \colon \nu \in G)$. Note that L does not depend on the chosen Weierstrass model for E, since changing the Weierstrass model, the invariant differential ω_E changes by a K-multiple. On the other hand, it is not hard to check that replacing E with a K-isogenous curve the quantity λ_ν changes by a K-multiple, and this proves that L depends only on the K-isogeny class of E.

Let us prove that L is Galois over $\mathbb{Q}$. By Lemma 3.3.1, this amounts to proving that ${}^\sigma\lambda_\nu \in L$ for every $\sigma \in G_\mathbb{Q}$. Let $\sigma \in G_\mathbb{Q}$ and $\nu \in G$ and consider the isogeny ${}^\sigma\mu_\nu \colon {}^{\overline{\sigma}\nu}E \to {}^{\overline{\sigma}}E$. Here $\overline{\sigma}$ is the class of σ in G. Note that $\mu_{\overline{\sigma}}{}^\sigma\mu_\nu \in \mathrm{Hom}_{\overline{\mathbb{Q}}}({}^{\overline{\sigma}\nu}E, E)$, and therefore there exists a non-zero integer m such that $\mu_{\overline{\sigma}}{}^\sigma\mu_\nu = m \cdot \mu_{\overline{\sigma}\nu}$. Looking at the action on differentials, we get that ${}^\sigma\lambda_\nu\lambda_{\overline{\sigma}} = m\lambda_{\overline{\sigma}\nu}$. This shows that ${}^\sigma\lambda_\nu \in L$, and since σ and ν were arbitrary, the claim follows.

The facts that $\mathrm{Gal}(L/K)$ has exponent 2 and that E is completely defined over L are clear from the construction of L.

Finally, let M be a number field containing K and such that E is completely defined over M. Let $\nu \in G$ and let $\mu \colon {}^\nu E \to E$ be an isogeny defined over M. Then $\mu = m\mu_\nu$ for some non-zero $m \in \mathbb{Z}$. Since μ is defined over M, by looking at the action of μ on invariant differentials, we see that $m\lambda_\nu = m^\sigma\lambda_\nu$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/M)$. Thus, $\lambda_\nu \in M$ for every ν, and this shows that $L \subseteq M$. □

Definition 3.3.3. The number field L determined by Proposition 3.3.2 is called the *minimal field of complete definition* of E.

3.4 Descent up to isogeny

In the philosophy of studying L-functions, it is important to understand when an elliptic curve "comes" from a subfield. For example, as we have seen in chapter 2, if E is an elliptic curve over $\mathbb{Q}$ and K is a quadratic number field, the L-function of E_K is simpler to study than the L-function of a $\mathbb{Q}$-curve over K which is not isogenous to an elliptic curve over $\mathbb{Q}$. This motivates the following definition.

Definition 3.4.1. Let E be a $\mathbb{Q}$-curve completely defined over a number field L, and let K be a subfield of L which is Galois over $\mathbb{Q}$. We say that E is *inflated from* K if there exists a $\mathbb{Q}$-curve C completely defined over K such that E is L-isogenous to C_L. If this is not the case, we say that E is *primitive*.

The reason for the terminology "inflated" will be clarified by Proposition 3.4.4.

In this section, we are going to deduce from the following theorem a criterion which allows us to decide when a $\mathbb{Q}$-curve completely defined over a Galois number field is inflated from a smaller field.

Theorem 3.4.2 ([62, Theorem 8.2])**.** Let L/K be a Galois extension of number fields, and let E be a $\mathbb{Q}$-curve completely defined over L. Then the following are equivalent:

i) there exist isomorphisms $\mu_\sigma\colon {}^\sigma E \to E$ of elliptic curves up to isogeny over L such that

$$\mu_\sigma {}^\sigma\mu_\tau = \mu_{\sigma\tau} \qquad \text{for all } \sigma \in \mathrm{Gal}(L/K);$$

ii) there exists an elliptic curve C defined over K such that E is L-isogenous to C_L.

Remark 3.4.3. Assume that $L/\mathbb{Q}$ is Galois. Then condition i) can be restated in the following form:

$$[\xi_L(E)] \in \ker(\mathrm{Res}^L_K\colon H^2(L/\mathbb{Q},\mathbb{Q}^*) \to H^2(L/K,\mathbb{Q}^*)).$$

Proposition 3.4.4. Let E be a $\mathbb{Q}$-curve without CM completely defined over a Galois number field L and let $\xi_L(E)$ be its associated 2-cocycle. Let $K \subseteq L$ be a subfield which is Galois over $\mathbb{Q}$ and assume that $\mathrm{Gal}(L/K)$ is contained in the center of $\mathrm{Gal}(L/\mathbb{Q})$. Then the following are equivalent:

i) E is inflated from K;

ii) $[\xi_L(E)] \in \mathrm{Im}(\mathrm{Inf}^K_L\colon H^2(K/\mathbb{Q},\mathbb{Q}^*) \to H^2(L/\mathbb{Q},\mathbb{Q}^*))$.

Proof. First assume i). Let C be a $\mathbb{Q}$-curve completely defined over K such that $C_L \sim E$. For all $\overline{\sigma} \in \mathrm{Gal}(K/\mathbb{Q})$, let us fix a K-isogeny $\mu_{\overline{\sigma}}\colon {}^{\overline{\sigma}}C \to C$. Let $\xi_K(C) \in Z^2(K/\mathbb{Q},\mathbb{Q}^*)$ be the 2-cocycle attached to C/K via the system of isogenies $\{\mu_{\overline{\sigma}}\}_{\overline{\sigma}}$, so that $\xi_K(C)(\overline{\sigma},\overline{\tau}) = \mu_{\overline{\sigma}}{}^{\overline{\sigma}}\mu_{\overline{\tau}}\mu_{\overline{\sigma\tau}}^{-1}$. Now for every $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, let us set $\mu_\sigma = \mu_{\overline{\sigma}}\colon {}^\sigma C_L \to C_L$, for $\overline{\sigma}$ the class of σ in $\mathrm{Gal}(K/\mathbb{Q})$. Then a representative for the cocycle class attached to C_L is given by $\xi_L(C_L)(\sigma,\tau) = \mu_{\overline{\sigma}}{}^\sigma\mu_{\overline{\tau}}\mu_{\overline{\sigma\tau}}^{-1}$. Since C is completely defined over K, so is $\mu_{\overline{\tau}}$ for all $\tau \in \mathrm{Gal}(L/\mathbb{Q})$. Therefore $\mathrm{Gal}(L/K)$ acts trivially on $\mu_{\overline{\tau}}$ and thus

$$\xi_L(C_L)(\sigma,\tau) = \mu_{\overline{\sigma}}{}^{\overline{\sigma}}\mu_{\overline{\tau}}\mu_{\overline{\sigma\tau}}^{-1} = \xi_K(C)(\overline{\sigma},\overline{\tau}).$$

This shows that $[\xi_L(C_L)]$ is the inflation of $[\xi_K(C)]$, and since C_L and E are L-isogenous, we have that $[\xi_L(C_L)] = [\xi_L(E)]$ and the claim follows.

Now assume ii). Since $\mathrm{Res}^L_K \circ \mathrm{Inf}^K_L = 0$, we have $[\xi_L(E)] \in \ker(\mathrm{Res}^L_K)$. Thus by Theorem 3.4.2 there exists a $\mathbb{Q}$-curve C over K such that C_L is L-isogenous to E. Choose a system of isogenies $\{\mu_\sigma\colon {}^\sigma C_L \to C_L\}_{\sigma\in\mathrm{Gal}(L/\mathbb{Q})}$ with the following properties:

- $\mu_\sigma = 1$ whenever $\sigma \in \mathrm{Gal}(L/K)$;
- $\mu_\sigma = \mu_\tau$ whenever $\sigma \equiv \tau \bmod \mathrm{Gal}(L/K)$.

Let $\xi_L(C_L)$ be the 2-cocycle attached to C_L via the above system of isogenies. Now suppose that C is not completely defined over K. Then there exist $\nu \in \mathrm{Gal}(L/\mathbb{Q})$, $\vartheta \in \mathrm{Gal}(L/K)$ such that ${}^\vartheta\mu_\nu = -\mu_\nu$; this implies that

$$\xi_L(C_L)(\vartheta,\nu) = -1 \text{ and } \xi_L(C_L)(\nu,\vartheta) = 1. \tag{3.2}$$

On the other hand, by hypothesis $[\xi_L(C_L)] = [\xi_L(E)]$ is inflated, so there exists a cocycle $c \in Z^2(K/\mathbb{Q},\mathbb{Q}^*)$ such that $[\xi_L(C_L)] = \mathrm{Inf}^K_L([c])$. Let $\widetilde{c} \in Z^2(L/\mathbb{Q},\mathbb{Q}^*)$ be the cocycle defined by $\widetilde{c}(\sigma,\tau) = c(\overline{\sigma},\overline{\tau})$ for all $\sigma,\tau \in \mathrm{Gal}(L/\mathbb{Q})$, where $\bar{\cdot}$ denotes the class modulo $\mathrm{Gal}(L/K)$. Let $\alpha\colon \mathrm{Gal}(L/\mathbb{Q}) \to \mathbb{Q}^*$ be a map such that

$$\widetilde{c} = \xi_L(C_L) \cdot \delta\alpha.$$

Note that the cocycle condition for c implies that $c(1,\nu) = c(\nu,1)$ for every $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Thus, $\widetilde{c}(\nu,\vartheta) = \widetilde{c}(\vartheta,\nu)$ and by (3.2), this yields $\alpha(\nu\vartheta) = -\alpha(\vartheta\nu)$, a contradiction since $\nu\vartheta = \vartheta\nu$. □

Remark 3.4.5. Since the inflation map respects the decomposition of $H^2(K/\mathbb{Q}, \mathbb{Q}^*)$ in its sign and degree components, condition ii) of the proposition is equivalent to:

ii′)
$$[\xi_L(E)^{\pm}] \in \mathrm{Im}(\mathrm{Inf}_L^K \colon H^2(K/\mathbb{Q}, \{\pm 1\}) \to H^2(L/\mathbb{Q}, \{\pm 1\}))$$
and
$$[\xi_L(E)^{\deg}] \in \mathrm{Im}(\mathrm{Inf}_L^K \colon H^2(K/\mathbb{Q}, \mathbb{Q}_+^*) \to H^2(L/\mathbb{Q}, \mathbb{Q}_+^*)).$$

3.5 Quadratic twists of quadratic $\mathbb{Q}$-curves

Our goal in this section is to understand under which conditions a quadratic $\mathbb{Q}$-curve admits strongly modular quadratic twists over its minimal field of complete definition. Let $d \neq 1$ be a squarefree integer and let $K = \mathbb{Q}(\sqrt{d})$ with $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \nu\}$. Let E be a $\mathbb{Q}$-curve over K without CM. Let $\mu_\nu \colon {}^\nu E \to E$ be an isogeny, and assume that μ_ν cannot be defined over K. In such a situation the curve E is not strongly modular over K, because of Theorem 3.2.1.

Lemma 3.5.1. The minimal field L of complete definition of E has Galois group $C_2 \times C_2$.

Proof. It is clear from the construction of L in the proof of Proposition 3.3.2 that L is a quadratic extension of K.

Suppose that $\mathrm{Gal}(L/\mathbb{Q}) \simeq C_4$. Let $\mathrm{Gal}(L/\mathbb{Q}) = \{1, \nu, \nu^2, \nu^3\}$, where by a slight abuse of notation, $\nu \in \mathrm{Gal}(L/\mathbb{Q})$ is a lift of $\nu \in \mathrm{Gal}(K/\mathbb{Q})$. Let us try to describe the cocycle $\xi_L^{\pm}$ attached to E_L. Since $H^2(C_4, \{\pm 1\}) \simeq C_2 \simeq H_s^2(C_4, \{\pm 1\})$, the cocycle $\xi_L^{\pm}$ must be symmetric. Let $\mu_\nu \colon {}^\nu E \to E$ be an isogeny. We can set $\mu_{\nu^2} = \mathrm{id}$ and $\mu_{\nu^3} = \mu_\nu$. Then $\xi_L^{\pm}(\nu, \nu^2) = \mu_\nu {}^\nu\mu_{\nu^2} \mu_{\nu^3}^{-1} = \mu_\nu \mu_\nu^{-1} = 1$. On the other hand, note that ${}^{\nu^2}\mu_\nu$, which is an isogeny ${}^\nu E \to E$, cannot coincide with μ_ν, since this would imply that μ_ν is defined over K. But μ_ν and ${}^{\nu^2}\mu_\nu$ have the same degree, and therefore ${}^{\nu^2}\mu_\nu = -\mu_\nu$. Thus $\xi_L^{\pm}(\nu^2, \nu) = \mu_{\nu^2} {}^{\nu^2}\mu_\nu \mu_{\nu^3}^{-1} = -\mu_\nu \mu_\nu^{-1} = -1$, which contradicts the symmetry of $\xi_L^{\pm}$. □

Let $e \neq 0, 1$ be a squarefree integer such that $L = \mathbb{Q}(\sqrt{d}, \sqrt{e})$. From now on, we set
$$K_e \coloneqq \mathbb{Q}(\sqrt{e}), \quad K_{de} \coloneqq \mathbb{Q}(\sqrt{de}) \text{ and } G \coloneqq \mathrm{Gal}(L/\mathbb{Q}) = \{1, \nu, \vartheta, \nu\vartheta\},$$
where ϑ is the generator of $\mathrm{Gal}(L/K)$ and by a small abuse of notation the element $\nu \in G$ restricts to the non-trivial automorphism of K which we also call ν.

Let us compute the 2-cocycle attached to E_L. Let μ_ϑ be the identity ${}^\vartheta E_L = E_L \to E_L$ and let $\mu_{\nu\vartheta} = \mu_\nu \colon {}^{\nu\vartheta}E_L = {}^\nu E_L \to E_L$. Note that ${}^\vartheta\mu_\nu$ is an isogeny ${}^{\nu\vartheta}E_L = {}^\nu E_L \to E_L = {}^\vartheta E_L$ with the same degree of μ_ν and since E_L has no CM, ${}^\vartheta\mu_\nu$ has to coincide with μ_ν up to sign. However if it were ${}^\vartheta\mu_\nu = \mu_\nu$ then μ_ν would be defined over K, which is a contradiction. Therefore ${}^\vartheta\mu_\nu = -\mu_\nu$. Analogously, ${}^{\nu\vartheta}\mu_\nu = -{}^\nu\mu_\nu$. The isogeny $\mu_\nu {}^\nu\mu_\nu$ coincides with multiplication by an integer $m \in \mathbb{Z} \setminus \{0, 1\}$. By an easy computation we end up with the following table for the cocycle $\xi_L \coloneqq \xi_L(E_L)$.

$\xi_L(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	1	-1	-1
ν	1	1	m	m
$\nu\vartheta$	1	1	$-m$	$-m$

The above table shows that the curve E_L is not strongly modular over L, because of Theorem 3.2.1. The question we want to address is: which quadratic twists of E_L are strongly modular? A first answer is provided by the following proposition.

Proposition 3.5.2. Let $\lambda \in L^*$. Then the twisted curve $E_L^{(\lambda)}$ is strongly modular over L if and only if $L(\sqrt{\lambda})$ is Galois over $\mathbb{Q}$ and $\mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q})$ is non-abelian. Moreover, in this case the cohomology class $[\xi_L^\lambda]$ attached to $E_L^{(\lambda)}$ becomes trivial in $H^2(L/\mathbb{Q}, \overline{\mathbb{Q}}^*)$.

Proof. By Theorem 3.2.1, $E_L^{(\lambda)}$ is strongly modular precisely when its attached cocycle ξ_L^λ is symmetric. Recall that by Remark 3.2.3 this is equivalent to asking that $[(\xi_L^\lambda)^\pm] \in H_s^2(L/\mathbb{Q}, \{\pm 1\})$.

Let $\lambda \in L^*$ be such that $L(\sqrt{\lambda})$ is Galois over $\mathbb{Q}$. Let $A \coloneqq \mathrm{Gal}(L(\sqrt{\lambda})/L) \simeq \{\pm 1\}$, $\widetilde{G} \coloneqq \mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q})$ and $G = \mathrm{Gal}(L/\mathbb{Q})$. We have that $\widetilde{G}$ is abelian if and only if the 2-cocycle attached to the exact sequence $1 \to A \to \widetilde{G} \to G \to 1$ is symmetric. Therefore when $\widetilde{G}$ is abelian, by Lemma 3.2.2 it follows that the symmetry of the cocycle ξ_L attached to E_L does not change under twisting by λ, and this shows that $E_L^{(\lambda)}$ cannot be strongly modular. On the other hand, note that by Lemma 3.1.7 we have that $H_s^2(G, A) \simeq C_2 \times C_2$ and by Corollary 3.1.10 $H^2(G, A) \simeq C_2^3$. This shows that $H^2(G, A)/H_s^2(G, A) \simeq C_2$, which means that the the product of two non-symmetric cocycle classes in $H^2(G, A)$ is symmetric and therefore whenever $\widetilde{G}$ is non-abelian, and so its attached cocycle is not symmetric, then $[\xi_L^\lambda] \in H_s^2(G, A)$.

The second assertion follows directly from Corollary 3.1.8. □

Remark 3.5.3. Let us describe the structure of $H^2(L/\mathbb{Q}, \{\pm 1\})$ in more detail. Recall that elements of this group correspond to equivalence classes of central group extensions of the form $1 \to \{\pm 1\} \to \widetilde{G} \to G \to 1$. There are four symmetric cocycles classes and four non-symmetric ones. The symmetric cocycle classes correspond to group extensions with $\widetilde{G} \simeq C_2 \times C_2 \times C_2$ or $\widetilde{G} \simeq C_4 \times C_2$. The non-symmetric cocycle classes correspond to group extensions with $\widetilde{G} \simeq D_4$ or $\widetilde{G} \simeq H_8$. All extensions with $\widetilde{G} \simeq H_8$ are equivalent to each other, while there are three non-equivalent extensions with $\widetilde{G} \simeq D_4$. These are uniquely determined by the image in G of the subgroup of order 4 in D_4. If $\lambda \in L^*$ is such that $\widetilde{G} = \mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q}) \simeq D_4$, $\sigma \in \widetilde{G}$ is an element of order 4 and $\overline{\sigma}$ is its image in G, then $L^{\overline{\sigma}}$ is the unique subextension such that $\mathrm{Gal}(L(\sqrt{\lambda})/L^{\overline{\sigma}}) \simeq C_4$.

3.5.1 Inflated and primitive twists

Let $\lambda \in L$ be such that $E_L^{(\lambda)}$ is strongly modular, and let $\xi_L^\lambda \in Z^2(G, \mathbb{Q}^*)$ be the associated cocycle, which is symmetric. By Proposition 3.4.4 and Remark 3.4.5, E_L is inflated from a Galois subfield $F \subseteq L$ if and only if $[\xi_L^{\lambda,\pm}]$ is the inflation of a cohomology class in $H^2(F/\mathbb{Q}, \{\pm 1\})$ and $[\xi_L^{\lambda,\deg}]$ is the inflation of a cohomology class in $H^2(F/\mathbb{Q}, \mathbb{Q}_+^*)$. Moreover, since the inflation of a cohomology class c is symmetric if and only if c is itself symmetric, we can replace every cohomology group we are dealing with with its subgroup of symmetric classes.

In the next two lemmas we will describe necessary and sufficient conditions for $E_L^{(\lambda)}$ to be inflated.

Lemma 3.5.4. If $|m| \in (\mathbb{Q}^*)^2$, then E_L is an inflated $\mathbb{Q}$-curve.

Proof. If $|m| \in (\mathbb{Q}^*)^2$ then the degree component of $[\xi_L]$ is trivial, and so the same is true for the degree component of $[\xi_L^\lambda]$. Therefore it is enough to show that the sign component of $[\xi_L^\lambda]$ is inflated from $H_s^2(F/\mathbb{Q}, \{\pm 1\})$ for some Galois subfield $F \subseteq L$. Now the claim follows simply by listing elements of $H_s^2(L/\mathbb{Q}, \{\pm 1\})$; these are represented by the cocycles $\{1, b_1, b_2, b_3\}$ where:

$b_1(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	1	1	1
ν	1	1	-1	-1
$\nu\vartheta$	1	1	-1	-1

$b_2(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	-1	1	-1
ν	1	1	1	1
$\nu\vartheta$	1	-1	1	-1

$b_3(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	-1	-1	1
ν	1	-1	-1	1
$\nu\vartheta$	1	1	1	1

Obviously the trivial class in $H_s^2(L/\mathbb{Q}, \{\pm 1\})$ is the inflation of the trivial class in $H^2(\{1\}, \{\pm 1\})$ so $[\xi_L^\lambda]$ is trivial if and only if $E^{(\lambda)}$ is L-isogenous to an elliptic curve defined over $\mathbb{Q}$. Beyond that, each b_i is the inflation of the cocycle

$c_i(\cdot,\cdot)$	1	σ_i
1	1	1
σ_i	1	-1

where for $i = 1, 2, 3$ the element σ_i is a generator respectively of $\mathrm{Gal}(K/\mathbb{Q}), \mathrm{Gal}(K_e/\mathbb{Q})$ and $\mathrm{Gal}(K_{de}/\mathbb{Q})$. □

Lemma 3.5.5. Suppose $|m| \notin (\mathbb{Q}^*)^2$. Then $E_L^{(\lambda)}$ is inflated from K if and only if $\mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q}) \simeq D_4$ and the unique C_4-subextension of $L(\sqrt{\lambda})$ is L/K_e or L/K_{de}. Consequently, $E_L^{(\lambda)}$ is primitive over L if and only if either $\mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q}) \simeq H_8$ or $\mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q}) \simeq D_4$ and $\mathrm{Gal}(L(\sqrt{\lambda})/K) \simeq C_4$.

Proof. The degree component of ξ_L coincides with that of ξ_L^λ and is represented by the following cocycle:

$\xi_L^{\deg}(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	1	1	1
ν	1	1	$\lvert m\rvert$	$\lvert m\rvert$
$\nu\vartheta$	1	1	$\lvert m\rvert$	$\lvert m\rvert$

It is immediate to see that this cocycle is the inflation from $H^2(K/\mathbb{Q}, \mathbb{Q}_+^*)$ of the cohomology class $[c]$, where $c(1,1) = c(1,\nu) = c(\nu,1) = 1$ and $c(\nu,\nu) = |m|$, while it is not the inflation of a class lying in $H^2(F/\mathbb{Q}, \mathbb{Q}_+^*)$ for any $F \in \{\mathbb{Q}, K_e, K_{de}\}$. Thus if $E_L^{(\lambda)}$ is inflated, it is inflated from K.

Therefore it is enough to understand when $[\xi_L^{\lambda,\pm}]$ is the inflation of a class in $H_s^2(K/\mathbb{Q}, \{\pm 1\})$. This group contains only two elements: the class of the trivial cocycle and the class $[c]$ where $c(1,1) = c(1,\nu) = c(\nu,1) = 1$ and $c(\nu,\nu) = -1$. The

inflation of the trivial class is of course trivial, while the inflation of the second one is represented by

$\widetilde{c}(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	1	1	1
ν	1	1	-1	-1
$\nu\vartheta$	1	1	-1	-1

Now the sign component of $[\xi_L]$ is represented by one of the following two non-cohomologous cocycles, depending on the sign of m:

$b_1(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	1	-1	-1
ν	1	1	1	1
$\nu\vartheta$	1	1	-1	-1

$b_2(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	1	-1	-1
ν	1	1	-1	-1
$\nu\vartheta$	1	1	1	1

Since $b_1 = \widetilde{c}\cdot b_2$, the class $[\xi_L^\lambda]$ is inflated precisely when the cohomology class attached to the exact sequence

$$1 \to \mathrm{Gal}(L(\sqrt{\lambda})/L) \simeq \{\pm 1\} \to \mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q}) \to 1 \tag{3.3}$$

is either $[b_1]$ or $[b_2]$.

The key observation is now the following: the cohomology class in $H^2(L/\mathbb{Q},\{\pm 1\})$ associated to the exact sequence (3.3) coincides with (the inverse of) the element $\mathrm{trg}(b) \in H^2(L/\mathbb{Q},\{\pm 1\})$ obtained by applying the transgression map

$$\mathrm{trg}\colon H^1(L(\sqrt{\lambda})/L,\{\pm 1\}) \to H^2(L/\mathbb{Q},\{\pm 1\})$$

to the unique non-trivial element $b \in H^1(L(\sqrt{\lambda})/L,\{\pm 1\}) \simeq \mathrm{Hom}(C_2,\{\pm 1\}) = \{1,b\}$. This can be seen just by applying the definition of the two constructions explained in Remark 3.1.2 and Lemma 3.1.3.

Let $\lambda \in L$ be such that $\mathrm{Gal}(L(\sqrt{\lambda})/L) \simeq D_4 = \langle \sigma,\tau\colon \sigma^4 = \tau^2 = 1,\ \tau\sigma = \sigma^3\tau\rangle$.

Consider the exact sequence

$$1 \longrightarrow \mathrm{Gal}(L(\sqrt{\lambda})/L) \longrightarrow \mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q}) \xrightarrow{\pi_1} \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow 1,$$

where $\pi_1(\sigma) = \nu\vartheta$ and $\pi_1(\tau) = \nu$. This corresponds to the situation where $L(\sqrt{\lambda})/K_{de}$ is the unique C_4-subextension. Let us choose the following normalized section $\widetilde{\cdot}$ for π_1: $\widetilde{\vartheta} = \sigma\tau$, $\widetilde{\nu} = \tau$ and $\widetilde{\nu\vartheta} = \sigma$. Then $\mathrm{trg}(b)$ is represented by the following cocycle:

$\widetilde{b}(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	1	1	1
ν	1	-1	1	-1
$\nu\vartheta$	1	-1	1	-1

which is cohomologous to b_1 by multiplying it by the coboundary of the cochain given by $b(1) = 1$, $b(\nu) = b(\vartheta) = b(\nu\vartheta) = -1$.

Analogously, consider the exact sequence

$$1 \longrightarrow \mathrm{Gal}(L(\sqrt{\lambda})/L) \longrightarrow \mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q}) \xrightarrow{\pi_2} \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow 1,$$

where $\pi_2(\sigma) = \nu$ and $\pi_2(\tau) = \vartheta$. This corresponds to the situation where $L(\sqrt{\lambda})/K_e$ is the unique C_4-subextension. Choosing as a normalized section of π_2 the map given by $\widetilde{\vartheta} = \tau$, $\widetilde{\nu} = \sigma$ and $\widetilde{\nu\vartheta} = \tau\sigma$, one checks that

$\widetilde{b}(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	1	1	1
ν	1	-1	-1	1
$\nu\vartheta$	1	-1	-1	1

which shows that $\widetilde{b}$ is cohomologous to b_2 by choosing the same cochain as in the previous case. □

The next step is to give necessary and sufficient conditions for the existence of primitive or inflated twists of E_L.

First let us recall the following terminology.

Definition 3.5.6. Let p be a prime number and let L/K be a (not necessarily finite) Galois extension of fields with Galois G. Assume that K contains a p-th root of unity. Consider the following group extension

$$1 \to C_p \to \widetilde{G} \xrightarrow{\pi} G \to 1, \tag{3.4}$$

where C_p is a cyclic subgroup of order p contained in the center of $\widetilde{G}$. Then *solving the embedding problem* relative to the extension L/K and the group extension (3.4) means to find a Galois extension M/K such that $L \subseteq M$, $\mathrm{Gal}(M/K) \simeq \widetilde{G}$ and the restriction of an automorphism of $\widetilde{G}$ on L coincides with its image under π.

The group extension (3.4) defines an element of $H^2(G, C_p)$; since C_p can be identified with a subgroup of L^* there is a natural map $\varphi_L \colon H^2(G, C_p) \to H^2(G, L^*)$. Since we will not need any other case, from now on we will set $p = 2$.

The next lemma is proven in [40, pp. 826-827] for finite Galois extensions. For the sake of completeness we reprove it here in a slightly more general form, which we will need later, although no major modification is required.

Lemma 3.5.7. Let $c \in Z^2(G, \{\pm 1\})$ be the 2-cocycle corresponding to the exact sequence (3.4). Then the embedding problem relative to c has a solution if and only if $[c] \in \ker \varphi_L$.

Proof. By Lemma 3.3.1, quadratic extensions of L which are normal over K are in bijection with elements of $H^0(G, L^*/(L^*)^2)$ (with the natural Galois action). If $\lambda \in L^*$

and $\overline{\lambda} \in L^*/(L^*)^2$ is its equivalence class, the corresponding quadratic extension of L is simply $L(\sqrt{\lambda})$. Note that we have the following exact diagram:

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & & \downarrow & & & & \\ & & & & \{\pm 1\} & & & & \\ & & & & \downarrow & & & & \\ 1 & \longrightarrow & (L^*)^2 & \longrightarrow & L^* & \longrightarrow & L^*/(L^*)^2 & \longrightarrow & 1 \\ & & & & \downarrow & & & & \\ & & & & (L^*)^2 & & & & \\ & & & & \downarrow & & & & \\ & & & & 1 & & & & \end{array}$$

which gives, taking Galois cohomology, the exact diagram

$$\begin{array}{ccccc} H^0(G, L^*/(L^*)^2) & \xrightarrow{\psi} & H^1(G, (L^*)^2) & \longrightarrow & H^1(G, L^*) \\ & & \downarrow{\scriptstyle \delta} & & \\ & & H^2(G, \{\pm 1\}) & & \\ & & \downarrow{\scriptstyle \varphi_L} & & \\ & & H^2(G, L^*) & & \end{array}$$

where $H^1(G, L^*) = 0$ by Hilbert theorem 90. Now suppose that the embedding problem represented by c is solved by a Galois extension $L(\sqrt{\lambda})$ for some $\lambda \in L^*$. Let $\overline{\lambda} \in H^0(G, L^*/(L^*)^2)$ be the equivalence class of λ; then $\psi(\overline{\lambda})$ is represented by the map sending $\sigma \to \dfrac{{}^{\sigma}\lambda}{\lambda}$. Fixing a square root β_σ of $\dfrac{{}^{\sigma}\lambda}{\lambda}$ in L^* yields a 2-cocycle given by $c_{\overline{\lambda}}(\sigma, \tau) = \dfrac{\beta_\sigma {}^{\sigma}\beta_\tau}{\beta_{\sigma\tau}}$ for all $\sigma, \tau \in G$ which represents the class $\delta(\psi(\overline{\lambda}))$. One checks that c is cohomologous to $c_{\overline{\lambda}}$, which shows that if the embedding problem relative to c has a solution, then $\varphi_L([c]) = 0$.

Conversely, if $\varphi_L([c]) = 0$ then $[c]$ comes from an element in $H^1(G, (L^*)^2)$, and being ψ surjective we get that $[c] = \delta(\psi(\overline{\lambda}))$ for some λ, so that the embedding problem relative to c has a solution. □

From the above lemma it follows immediately that the solvability of the embedding problem given by extension (3.4) depends only on the equivalence class of the extension.

Let us now consider our setting where $F = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{d}, \sqrt{e})$ is a $C_2 \times C_2$ extension of $\mathbb{Q}$ and $G = \mathrm{Gal}(L/\mathbb{Q}) = \langle \nu, \vartheta \rangle$ where ${}^{\nu}\sqrt{d} = -\sqrt{d}$, ${}^{\vartheta}\sqrt{e} = -\sqrt{e}$. For $a, b \in \mathbb{Q}$, we will denote by (a, b) the quaternion algebra over $\mathbb{Q}$ with basis $\{1, i, j, ij\}$ such that $i^2 = a$, $j^2 = b$, $ij = -ji$. Recall that the *reduced discriminant* of a quaternion algebra B over $\mathbb{Q}$ is the product of the finite primes of $\mathbb{Q}$ where B ramifies. A quaternion algebra is trivial in $\mathrm{Br}(\mathbb{Q})$ if and only if it has reduced discriminant 1.

Theorem 3.5.8 ([40, Theorems 4 and 5])**.** The following hold:

i) Let $H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the group of quaternions. The embedding problem relative to $L/\mathbb{Q}$ and the group extension

$$1 \to C_2 \to H_8 \xrightarrow{\pi} G \to 1$$

is solvable if and only if $(d, de)(e, de)(d, e) = 1$ in $\mathrm{Br}(\mathbb{Q})$, if and only if there exist $v_1, v_2, v_3, w_1, w_2, w_3 \in \mathbb{Q}$ such that

$$\begin{cases} d = v_1^2 + v_2^2 + v_3^2 \\ e = w_1^2 + w_2^2 + w_3^2 \\ v_1 w_1 + v_2 w_2 + v_3 w_3 = 0. \end{cases}$$

In this case, setting $t = 1 + \dfrac{v_1}{\sqrt{d}} + \dfrac{w_3}{\sqrt{e}} + \dfrac{v_1 w_3 - v_3 w_1}{\sqrt{de}}$, the extensions solving the problem are exactly the ones of the form $L(\sqrt{qt})$, for $q \in \mathbb{Q}^*$.

ii) Let $D_4 = \langle \sigma, \tau \colon \sigma^4 = \tau^2 = 1,\ \sigma\tau = \tau\sigma^3 \rangle$ be the dihedral group of order 8. The embedding problem relative to $L/\mathbb{Q}$ and the group extension

$$1 \to C_2 \to D_4 \xrightarrow{\pi} G \to 1$$

where $\pi(\sigma) = \vartheta$ and $\pi(\tau) = \nu$ is solvable if and only if $(-d, e) = 1$ in $\mathrm{Br}(\mathbb{Q})$.

In this case, if $x, y \in \mathbb{Q}$ are such that $d = ey^2 - x^2$, the extensions solving this problem are exactly the ones of the form $L(\sqrt{q(ey + x\sqrt{e})})$ for $q \in \mathbb{Q}^*$.

Recall that E_L is a $\mathbb{Q}$-curve completely defined over L. We can deduce from Theorem 3.5.8 the following result.

Theorem 3.5.9. There exists $\lambda \in L^*$ such that $E^{(\lambda)}$ is strongly modular and primitive if and only if at least one of the following conditions is satisfied:

a) the quaternion algebra $(-d, -e)$ has reduced discriminant 2;

b) the quaternion algebra $(-d, e)$ is trivial in $\mathrm{Br}(\mathbb{Q})$.

More precisely, a) is satisfied if and only if there exists λ such that $\mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q}) \simeq H_8$, while b) is satisfied if and only if there exists λ such that $\mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q}) \simeq D_4$ and the C_4-subextension is $L(\sqrt{\lambda})/\mathbb{Q}(\sqrt{d})$.

There exists $\lambda \in L^*$ such that $E^{(\lambda)}$ is strongly modular and inflated from K if and only if at least one of the following holds:

c) the quaternion algebra $(d, -e)$ is trivial in $\mathrm{Br}(\mathbb{Q})$;

d) the quaternion algebra $(d, -de)$ is trivial in $\mathrm{Br}(\mathbb{Q})$.

More precisely, c) holds if and only if then there exists $\lambda \in L^*$ such that $\mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q}) \simeq D_4$ and the C_4-subextension is $L(\sqrt{\lambda})/K_e$, and d) holds if and only if there exists $\lambda \in L^*$ such that $\mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q}) \simeq D_4$ and the C_4-subextension is $L(\sqrt{\lambda})/K_{de}$.

Proof. By Proposition 3.5.2, $E^{(\lambda)}$ is strongly modular if and only if $\mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q})$ is non-abelian, so isomorphic to either D_4 or H_8. By Lemma 3.5.5, $E^{(\lambda)}$ is primitive over L if and only if either $\mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q}) \simeq H_8$ or $\mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q}) \simeq D_4$ and the C_4-subextension is $L(\sqrt{\lambda})/\mathbb{Q}(\sqrt{d})$ where $K = \mathbb{Q}(\sqrt{d})$. Therefore we just have to understand, using Theorem 3.5.8, when this is possible.

As noticed in [40, p. 239], case a) holds if and only if the quadratic forms $S_{d,e} = \frac{1}{de}X^2+dY^2+eZ^2$ and $T = X^2+Y^2+Z^2$ are equivalent over $\mathbb{Q}$. This implies immediately that $d, e > 0$ because $S_{d,e}$ and T must have the same signature. Since the rank and the discriminant obviously coincide, it only remains to check that the Hasse-Witt invariants coincide. If p is a prime the Hasse-Witt invariant of T at p is 1, while the Hasse-Witt invariant of $S_{d,e}$ at p is given by

$$(de,d)_p(de,e)_p(d,e)_p = (de,d)_p(de,e)_p(-d,-e)_p(d,-1)_p(-1,e)_p(-1,-1)_p =$$

$$= (de,-de)_p(-d,-e)_p(-1,-1)_p = (-d,-e)_p(-1,-1)_p,$$

where we used bilinearity of the Hilbert symbol and the fact that $(a,-a)_p = 1$ for every $a \in \mathbb{Q}^*$ and every prime p. Now the claim follows from the fact that $(-1,-1)$ ramifies precisely at 2 and ∞.

Case b), c) and d) follow easily from point ii) of Theorem 3.5.8. □

Corollary 3.5.10. The curve E has a strongly modular quadratic twist over K if and only if the curve E_L has a strongly modular twist which is inflated from K.

Proof. First recall that, by Theorem 3.2.1, a $\mathbb{Q}$-curve defined over a quadratic field K is strongly modular if and only if it is completely defined over K.

Let $\lambda \in K^*$ be such that $E^{(\lambda)}$ is strongly modular over K. Then the base-changed curve $(E^{(\lambda)})_L$ is strongly modular over L because its attached cocycle is the inflation of a symmetric one, and is therefore symmetric. On the other hand, $(E^{(\lambda)})_L$ is L-isomorphic to $(E_L)^{(\lambda)}$ and therefore E_L has a strongly modular twist inflated from K.

Conversely, if E_L has a strongly modular twist $(E_L)^{(\lambda)}$ inflated from K, then by Theorem 3.5.9 we have that $(d,-e)$ or $(d,-de)$ is trivial. Theorem 3.5.8 shows that we can choose $\lambda \in K^*$: it is enough to use point ii) of the theorem replacing the map π by the one given by $\pi(\tau) = \vartheta$ and $\pi(\sigma) = \nu$ or $\pi(\sigma) = \nu\vartheta$. Then d plays the role of e in the notation of the theorem and it is clear that $\lambda \in K^*$. Therefore $(E_L)^{(\lambda)}$ is L-isomorphic to $(E^{(\lambda)})_L$. If $E^{(\lambda)}$ is not defined over K, then E_L is not strongly modular because, as the computation in section 3.5 shows, its attached cocycle would not be symmetric. Therefore $E^{(\lambda)}$ is completely defined over K. □

3.5.2 Examples

In this section we will provide examples of $\mathbb{Q}$-curves with different behaviours with respect to the existence of primitive and inflated strong modular quadratic twists.

Example 1

Let us borrow the following example from [58]. Let E be the following elliptic curve without CM over $K = \mathbb{Q}(\sqrt{-3})$:

$$E\colon y^2 = x^3 + 2x^2 + bx,$$

where $b \in \mathcal{O}_K$ is any element of trace 1. There is an isogeny $\mu_\nu \colon {}^\nu E \to E$ such that $\mu_\nu {}^\nu\mu_\nu = -2$. The minimal field of definition of E is $L = \mathbb{Q}(\sqrt{-3}, \sqrt{-2})$. Since $(3, -2)$ is trivial in $\mathrm{Br}(\mathbb{Q})$, by Theorem 3.5.9 there are quadratic extensions of L of type D_4 over $\mathbb{Q}$ with C_4-subextension $L(\sqrt{\lambda})/K$. Since $\alpha = 1 + \sqrt{-2} \in \mathbb{Q}(\sqrt{e})$ has norm $3 = -d$, by Theorem 3.5.8 we know that the set of all these extension is $\left\{ L\left(\sqrt{r + r/\sqrt{-2}}\right) : r \in \mathbb{Q}^* \right\}$. The one found in [58] corresponds to $r = 2$. Let $\lambda = 2 - \sqrt{-2}$. An integral model for $E_L^{(\lambda)}$ is given by

$$E_L^{(\lambda)} \colon y^2 = x^3 + (4 - 2\sqrt{-2})x^2 + b(2 - 4\sqrt{-2})x.$$

By Theorem 3.5.9 there are no quadratic extensions of L which are of type H_8 over $\mathbb{Q}$, nor quadratic extension of type D_4 with C_4-subextension $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{6})$. Thus, all strongly modular quadratic twists of E are primitive over L. Note also that [58, Proposition 6.2], which asserts that no quadratic twists of E are completely defined over K, follows easily from Corollary 3.5.10.

To construct other examples, consider the following family of $\mathbb{Q}$-curves given in [59]:

$$E_a \colon y^2 = x^3 - 3\sqrt{a}(4 + 5\sqrt{a})x + 2\sqrt{a}(2 + 14\sqrt{a} + 11a),$$

where $a \in \mathbb{Z}$ is not a square. Every E_a is defined over $K_a \coloneqq \mathbb{Q}(\sqrt{a})$ but its minimal field of complete definition is $L_a \coloneqq K_a(\sqrt{3})$.

We remark that E_a has positive algebraic rank for every a: the point $P_a \coloneqq (1 + 2\sqrt{a}, 1 - \sqrt{a})$ belongs $E_a(K_a)$ and

$$2P_a = \left(\frac{1 + 9a}{4} + \frac{1}{2}\sqrt{a}, \frac{1 - 9a}{8} + \frac{-27a + 35}{8}\sqrt{a} \right);$$

thus by the Nagell-Lutz theorem (see for example [43, Theorem III.2.1]), P_a has infinite order. In future work, it might be interesting to investigate how the rank of a fixed E_a varies in families of strongly modular twists.

Example 2

Consider the curve $(E_6)_{L_6}$. With the notation of Theorem 3.5.9 we have that $d = 6$ and $e = 3$. Since $j(E_6) = \dfrac{27625536}{125} + \dfrac{10768896}{125}\sqrt{6}$, it follows that E_6 has no CM.

The quaternion algebra $(-6, -3) = (-2, -3)$ has reduced discriminant 2 and therefore by Theorem 3.5.9 it follows that L_6 has a quadratic extension which is of H_8-type over $\mathbb{Q}$. Following the notation of Theorem 3.5.8 we can pick $v_1 = 2$, $v_2 = v_3 = 1$, w_1 and $w_2 = w_3 = -1$. Thus $t = 1 + \dfrac{2}{\sqrt{6}} - \dfrac{1}{\sqrt{3}} - \dfrac{1}{\sqrt{2}}$ and all H_8-type extensions of L_6 are given by $L_6(\sqrt{qt})$ for $q \in \mathbb{Q}^*$. For example, letting $q = 1$ and $\lambda = t$, an integral model for $(E_6)_{L_6}^{(\lambda)}$ is given by

$$(E_6)_{L_6}^{(\lambda)} \colon y^2 = x^3 + Ax + B,$$

where

$$A = 4080384\alpha^3 - 13616640\alpha^2 - 412416\alpha + 1375488,$$

$$B = -25868537856\alpha^3 + 82215567360\alpha^2 + 2613252096\alpha - 8305459200$$

and $\alpha = \sqrt{2} + \sqrt{3}$. This is a primitive strongly modular curve over L_6.

Since $(-6, 3)$ and $(6, -3)$ both have reduced discriminant 6, there are no extensions of L_6 which are of D_4-type over $\mathbb{Q}$ with C_4-subextension $L_6/\mathbb{Q}(\sqrt{6})$ or $L_6/\mathbb{Q}(\sqrt{3})$. On the other hand, $(6, -18)$ is trivial in $\mathrm{Br}(\mathbb{Q})$, so by Corollary 3.5.10 there exist strongly modular twists of E_6. To find them, notice that by Theorem 3.5.8 it is enough to find $x, y \in \mathbb{Q}$ with $6y^2 - x^2 = 18$. As $x = 6$, $y = 3$ solve this equation, letting $t = 18 + 6\sqrt{6}$ we get that all extensions of L_6 of type D_4 over $\mathbb{Q}$ are given by $L_6(\sqrt{qt})$, for $q \in \mathbb{Q}^*$. Let us choose for example $q = 1/6$ and $\lambda' = qt$. Then an integral model for $E_6^{(\lambda')}$ is

$$E_6^{(\lambda')} : y^2 = x^3 - (28512 + 11520\sqrt{6})x + 2594304 + 1059840\sqrt{6}.$$

One can show, using the algorithm in [72], that E_6 has algebraic rank 1, while the curve $E_6^{(\lambda)}$ has algebraic rank 2. Two independent points of infinite order are given by

$$Q = \left(\frac{260}{3} + \frac{80}{3}\sqrt{6}, 120 + \frac{592}{9}\sqrt{6}\right)$$

and

$$R = \left(-\frac{4359264}{94249} - \frac{1341924}{94249}\sqrt{6}, \frac{44171464512}{28934443} + \frac{17910346128}{28934443}\sqrt{6}\right).$$

Example 3

The curve E_7 is not strongly modular, but since $(7, -3)$ is trivial, by Corollary 3.5.10 it has strongly modular quadratic twists. For example setting $\lambda = 7 + 2\sqrt{7}$, the curve $E^{(\lambda)}$ is strongly modular over K_7. An integral model is given by

$$E_7^{(\lambda)} : y^2 = x^3 - (166992 + 61824\sqrt{7})x + 36452864 + 13804672\sqrt{7}.$$

Again, E_7 has rank 1. On the other hand, $E_7^{(\lambda)}$ has rank 0; in fact $E_7^{(\lambda)}(K) = \{O\}$.

Since $(-7, -3)$ has reduced discriminant 3 and $(-7, 3)$ has reduced discriminant 21, Theorem 3.5.9 shows that $(E_7)_{L_7}$ has no primitive strongly modular twists.

Example 4

Finally, the curve $(E_5)_{L_5}$ has no strongly modular twists at all, since $(3, -5)$ has reduced discriminant 10, $(-3, -5)$ has reduced discriminant 5 and both $(5, -3)$ and $(5, -15)$ have reduced discriminant 15.

3.5.3 The abelian variety attached to $E^{(\lambda)}$

When $\lambda \in L$ such that $E_L^{(\lambda)}$ is strongly modular and primitive, the abelian variety $\mathrm{Res}_{L/\mathbb{Q}}(E_L^{(\lambda)})$ is modular and, as we will see below, simple. This situation can be seen in some sense as the mildest possible generalization of the one studied in chapter 2, since being $H^2(C_3, \{\pm 1\})$ trivial there are no primitive strongly modular $\mathbb{Q}$-curves over Galois number fields of degree 3. In what follows, we will deduce from the properties of $E_L^{(\lambda)}$ some of the properties of the corresponding newform.

Let $\lambda \in L$ such that $E_L^{(\lambda)}$ is strongly modular and primitive. Since in this section we will only deal with $E_L^{(\lambda)}$ for a fixed λ, in order to simplify the notation we will just

write E for $E_L^{(\lambda)}$ and ξ for ξ_L^{λ}. There are only two possible cohomology classes for ξ, represented by the following non-cohomologous cocycles:

$c_1(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	-1	1	-1
ν	1	1	$-m$	$-m$
$\nu\vartheta$	1	-1	$-m$	m

$c_2(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	-1	-1	1
ν	1	-1	m	$-m$
$\nu\vartheta$	1	1	$-m$	$-m$

These correspond respectively to the case where $\mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q}) \simeq H_8$ and $\mathrm{Gal}(L(\sqrt{\lambda})/\mathbb{Q}) \simeq D_4$. In any case, the cocycle ξ becomes trivial in $H^2(L/\mathbb{Q}, \overline{\mathbb{Q}}^*)$. In fact one can check that the maps $\alpha_1, \alpha_2 \colon \mathrm{Gal}(L/\mathbb{Q}) \to \overline{\mathbb{Q}}^*$ defined below split c_1 and c_2, respectively.

σ	1	ϑ	ν	$\nu\vartheta$
$\alpha_1(\sigma)$	1	i	$-i\sqrt{m}$	$\sqrt{m}$

σ	1	ϑ	ν	$\nu\vartheta$
$\alpha_2(\sigma)$	1	i	$\sqrt{m}$	$-i\sqrt{m}$

Let α be a splitting map for ξ. The number field F generated by the values of α is $\mathbb{Q}(i, \sqrt{m})$. Let $B \coloneqq \mathrm{Res}_{L/\mathbb{Q}}(E)$ and $\mathcal{R} \coloneqq \mathrm{End}^0_{\mathbb{Q}}(B)$. As we have seen in the proof of Theorem 1.2.3, $\mathcal{R}$ is the 4-dimensional commutative $\mathbb{Q}$-algebra with basis $\{g_\sigma \colon \sigma \in \mathrm{Gal}(L/\mathbb{Q})\}$ and product given by $g_\sigma g_\tau = \xi(\sigma,\tau) g_{\sigma\tau}$; thus the surjective homomorphism of $\mathbb{Q}$-algebras

$$\mathcal{R} \to F$$

$$g_\sigma \mapsto \alpha(\sigma)$$

is an isomorphism. Therefore B is a $\mathbb{Q}$-simple abelian variety of GL_2-type. This shows that there exists a newform $f = \sum_{n=1}^{+\infty} a_n q^n \in S_2(\Gamma_1(N), \varepsilon)$ for some N, ε such that $F = \mathbb{Q}(a_n \colon n \in \mathbb{N})$ and $A_f \sim_{\mathbb{Q}} B$. Therefore

$$L(E/L, s) = L(B/\mathbb{Q}, s) = L(A_f/\mathbb{Q}, s) = \prod_\sigma L({}^\sigma f, s)$$

where σ runs over the set of embeddings $F \to \mathbb{C}$. The level N of f is determined as in section 2.4, namely we have that

$$N_{L/\mathbb{Q}}(\mathcal{N}_L(E))\Delta_L^2 = N^4,$$

where $\mathcal{N}_L(E)$ is the conductor of E and Δ_L is the discriminant of L.

Remark 3.5.11. It is not always the case that if E is a strongly modular, primitive $\mathbb{Q}$-curve over a number field L, then $\mathrm{Res}_{L/\mathbb{Q}}(E)$ is $\mathbb{Q}$-simple. Let us take the following example from [31]. Let $L = \mathbb{Q}(\alpha)$ where $\alpha^4 - 4\alpha^2 + 2 = 0$. This is a C_4-extension of $\mathbb{Q}$; let ν be a generator of the Galois group. Consider the following $\mathbb{Q}$-curve completely defined over L:

$$E \colon y^2 + (\alpha^3 - 2\alpha)xy + (\alpha^3 - 2\alpha)y =$$
$$= x^3 + (-\alpha^3 + 3\alpha)x^2 + (-4\alpha^3 + 3\alpha^2 + 14\alpha - 14)x + 5\alpha^3 - 4\alpha^2 - 16\alpha + 10.$$

There is an isogeny $\mu_\nu \colon {}^\nu E \to E$ of degree 2 and an isomorphism $\mu_{\nu^2} \colon {}^{\nu^2} E \to E$, thus we can set $\mu_{\nu^3} = {}^\nu\mu_{\nu^2}\mu_\nu$. We let $\xi \in Z^2(L/\mathbb{Q}, \mathbb{Q}^*)$ be the cocycle attached to E via the system of isogenies $\{\mathrm{id}, \mu_\nu, \mu_{\nu^2}, \mu_{\nu^3}\}$. Now note that $H^2(L/\mathbb{Q}, \{\pm 1\}) = H^2_s(L/\mathbb{Q}, \{\pm 1\}) \simeq$

$\{\pm 1\}$. The cohomology class corresponding to -1 is not inflated from any subfield of L, thus if E is an inflated $\mathbb{Q}$-curve, it is inflated from $\mathbb{Q}$. This means in particular that the cocycle $\xi^{\pm}$ attached to E is a coboundary. However, note that $\xi^{\pm}(1,1) = 1$ while one can compute that $\xi^{\pm}(\nu^2, \nu^2) = -1$. Thus there cannot be a splitting map α, since one should have $\xi^{\pm}(1,1) = \alpha(1) = 1$ and consequently $\xi^{\pm}(\nu^2, \nu^2) = \alpha(\nu^2)^2 = -1$. This proves that E is primitive. On the other hand,

$$\mathrm{Res}_{L/\mathbb{Q}}(E) \sim A_f \times A_{f\otimes\chi},$$

where

$$f = q + (i+1)q^3 + (i-1)q^5 - 2iq^7 - iq^9 + (i-1)q^{11} + O(q^{12})$$

is the unique (up to conjugation) newform in $S_2(\Gamma_1(64))$ with character of order 4 and conductor 16 and χ is the unique non-trivial quadratic character $\mathrm{Gal}(L/\mathbb{Q}) \to \mathbb{C}^*$.

From now on, we will think of F as a subfield of $\mathbb{C}$, implicitly fixing an embedding $F \to \mathbb{C}$. Let $\mathrm{Gal}(F/\mathbb{Q}) = \{1, \sigma_1, \sigma_2, \sigma_3\}$ where σ_1 is complex conjugation and σ_2 is the element defined by ${}^{\sigma_2}\sqrt{m} = -\sqrt{m}$ and ${}^{\sigma_2}i = i$. Note that since F is a CM field, complex conjugation in the Galois group of F does not depend on our fixed embedding $F \to \mathbb{C}$.

Since E is completely defined over L, all endomorphisms of B are defined over L and this is also the smallest field of definition for the endomorphisms of B, i.e. L is the splitting field of f. Recall that for every $j \in \{1,2,3\}$ there exists a Dirichlet character χ_j, which we can assume to be primitive, such that

$$ {}^{\sigma_j}a_p = \chi_j(p)a_p \tag{3.5}$$

for almost all primes p (i.e. for a set of primes of density 1). Since f does not have CM, such characters are unique. Note that by [9, Proposition 2.3.5], equation (3.5) holds for all primes $p \nmid N$ and the conductor of χ_j divides N for all j. The splitting field of f is L, and is given by $\overline{\mathbb{Q}}^{\cap_j \ker \chi_j}$. This shows that the χ_j's are either the trivial character or quadratic characters on $\mathrm{Gal}(L/\mathbb{Q})$. Moreover, recall that for all primes $p \nmid N$ we have that

$$ a_p = \varepsilon(p)\overline{a_p}. \tag{3.6}$$

This implies easily that $\chi_1 = \varepsilon$ as Dirichlet characters modulo N. By [60, Propositions 3.2 and 3.3], the fact that F is a CM field implies that ε is non-trivial, so it is quadratic since χ_1 can only be trivial or quadratic. Now equations (3.5) and (3.6) imply that for all primes $p \nmid N$ one has

$$ {}^{\sigma_2}a_p = \chi_2(p)\varepsilon(p)^{\sigma_1}a_p$$

and therefore

$$ {}^{\sigma_3}a_p = {}^{\sigma_1}\chi_2(p)\chi_1(p)a_p.$$

This shows that $\chi_3 = {}^{\sigma_1}\chi_2 \cdot \chi_1$ as characters of $G_{\mathbb{Q}}$. Thus if χ_2 is trivial we have that $\chi_1 = \chi_3$, but this would imply that $L = \overline{\mathbb{Q}}^{\ker \chi_1}$ which is a quadratic field, and this is a contradiction. Similarly χ_3 cannot be trivial, because it would imply that $\chi_2 = \chi_1$ and we would get a contradiction again. Therefore χ_1, χ_2 and χ_3 are pairwise distinct quadratic characters, and so they must be precisely the three distinct non-trivial quadratic characters on $\mathrm{Gal}(L/\mathbb{Q})$. Thus the set $\{\overline{\mathbb{Q}}^{\ker \chi_j} : j = 1,2,3\}$ coincides with $\{\mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt{e}), \mathbb{Q}(\sqrt{de})\}$.

3.6 Strongly modular $\mathbb{Q}$-curves up to isomorphism

As we have seen in the previous sections, quadratic $\mathbb{Q}$-curves over a quadratic field K might have no strongly modular twists, even when they are base-changed to a field of complete definition L. It is therefore natural to ask whether there always exist a field M containing K, possibly bigger than L, such that E_M has a strongly modular twist. In this section, we will characterize completely the class of $\mathbb{Q}$-curves which are geometrically isomorphic to a strongly modular one.

Remark 3.6.1. Notice that every $\mathbb{Q}$-curve is geometrically isogenous to a strongly modular one. In fact, suppose that E is a $\mathbb{Q}$-curve and let f be a newform such that there exists a modular parametrization $A_f \to E$. If L is the splitting field of f, it is proven in [30] that A_f is isogenous over L to E'^n for some $n \in \mathbb{N}$, where E' is a $\mathbb{Q}$-curve over L. Note that E is geometrically isogenous to E' by the uniqueness of the decomposition up to isogeny. By [31, Proposition 2], the abelian variety $\mathrm{Res}_{L/\mathbb{Q}}(E')$ is isogenous to a product of abelian varieties attached to newforms. Therefore E'/L is strongly modular.

The theorem we will prove is the following.

Theorem 3.6.2. Let E be a $\mathbb{Q}$-curve over a number field K, and assume that $K = \mathbb{Q}(j(E))$. Then E is $\overline{\mathbb{Q}}$-isomorphic to a strongly modular curve over some extension of K if and only if K is Galois and the minimal field of complete definition of E is abelian over $\mathbb{Q}$.

Since every elliptic curve over $\overline{\mathbb{Q}}$ is isomorphic to an elliptic curve over $\mathbb{Q}(j(E))$, the theorem above describes completely the class of $\mathbb{Q}$-curves isomorphic to a strongly modular one.

Remark 3.6.3. Using similar ideas to that of Example 2.3.4, it is easy to construct 1) an example of a $\mathbb{Q}$-curve whose j-invariant generates a non-Galois number field and 2) an example of a $\mathbb{Q}$-curve whose j-invariant generates a Galois number field and whose minimal field of complete definition is non-abelian. This shows that Theorem 3.6.2 is as sharp as possible. Let us exhibit two such examples.

1) Consider the elliptic curve $E'\colon y^2 = x^3 + x + 1$ over $\mathbb{Q}$. Let $K = \mathbb{Q}(\alpha)$, where α is a root of $x^3 + x + 1$. This is a non-Galois number field. The base-changed curve E'_K has a non-trivial 2-torsion point, namely $P = (\alpha, 0)$. Now let ϕ be the isogeny with kernel $\{O, P\}$ and let $E \coloneqq E'_K/\ker\phi$. A Weierstrass equation for E is given by:

$$E\colon y^2 = x^3 - (4 + 15\alpha^2)x + 22 + 14\alpha.$$

One can check that

$$j(E) = \frac{9580464}{961} + \frac{51659856}{961}\alpha + \frac{72060192}{961}\alpha^2 \notin \mathcal{O}_K,$$

so $\mathbb{Q}(j(E)) = K$ and E has no CM. Moreover, E is a $\mathbb{Q}$-curve: if L is the Galois closure of K, then E_L is L-isogenous to all its Galois conjugates, since by construction all of them are L-isogenous to E'_L.

2) Consider the elliptic curve $E'\colon y^2 = x^3+x^2-2x-1$ over $\mathbb{Q}$. Let $K = \mathbb{Q}(\alpha)$, where α is a root of x^3+x^2-2x-1. This time K is a Galois number field. Again, the point $P = (\alpha, 0)$ is a non-trivial 2-torsion point of the base-changed curve E'_K. If ϕ is the isogeny with kernel $\{O, P\}$, a Weierstrass equation for $E \coloneqq E'_K/\ker\phi$ is given by:

$$E\colon y^2 = x^3 + x^2 + (8 - 10\alpha - 15\alpha^2)x - 14 - 36\alpha - 5\alpha^2.$$

We have that $j(E) = 66240+208912\alpha+143392\alpha^2$ generates K and we checked using Sage [75] that E has no CM. Since K is Galois, E has full 2-torsion over K and thus it follows easily that E is a $\mathbb{Q}$-curve completely defined over K. Now consider the quadratic twist of E by α:

$$E^{(\alpha)}\colon y^2 = x^3 + 4\alpha x^2 + (80 - 80\alpha - 432\alpha^2)x + 448 - 1088\alpha - 4736\alpha^2.$$

Since $K(\sqrt{\alpha})$ is not Galois over $\mathbb{Q}$, by Lemma 3.2.2 the curve $E^{(\alpha)}$ is not completely defined over K. On the other hand, if N is the Galois closure of $K(\sqrt{\alpha})$, one can check that E is completely defined over N. Now N is a non-abelian number field of degree 12, it is generated by a root of the polynomial $x^{12} + 4x^{10} + 10x^8 + 34x^6 - 7x^4 + 98x^2 + 49$ and its Galois group is isomorphic to the alternating group on 4 letters A_4. Thus, there are no subfields of N which contain K and are Galois over $\mathbb{Q}$, because A_4 has no normal subgroups of order 2. This proves that N is the minimal field of definition of $E^{(\alpha)}$.

In order to prove Theorem 3.6.2, we need two preliminary results, which we will now state and prove.

The first one shows that a $\mathbb{Q}$-curve over a non-Galois number field cannot be strongly modular. Recall that by Proposition 1.3.4, a $\mathbb{Q}$-curve over a number field K is strongly modular if and only if $\mathrm{Res}_{K/\mathbb{Q}}(E)$ is an abelian variety of GL_2-type.

Proposition 3.6.4. Let E be a $\mathbb{Q}$-curve over a number field K. If E is strongly modular, then $K/\mathbb{Q}$ is Galois.

Proof. Let us start by fixing the notation. Let $B \coloneqq \mathrm{Res}_{K/\mathbb{Q}}(E)$ be the restriction of scalars of E. If E is strongly modular, there exist newforms $f_1, \ldots, f_n$ such that

$$B \sim \prod_{i=1}^{n} (A_{f_i})^{t_i},$$

where A_{f_i} and A_{f_j} are not isogenous whenever $i \neq j$ and the t_i's are positive integers. To ease the notation, we set $A_i \coloneqq A_{f_i}$. Let L_i be the splitting field of f_i, for $i \in \{1, \ldots, n\}$. Recall that this is an abelian number field, and it is the smallest field over which all endomorphisms of A_i are defined. Let L be the compositum of all the L_i's.

Recall that the universal property of the restriction of scalars implies that

$$\mathrm{Hom}_{\mathbb{Q}}(X, B) \simeq \mathrm{Hom}_K(X_K, E) \tag{3.7}$$

for every $\mathbb{Q}$-scheme X.

We divide the proof in two steps.

Step 1. The first claim we will prove is that L is a subfield of K, and so that E is the base change of a $\mathbb{Q}$-curve E_0 completely defined over L and B_K decomposes as $(E_0)^{[K\colon\mathbb{Q}]}$. This will be helpful in understanding the structure of $\mathrm{End}_{\mathbb{Q}}(B)$.

Notice that for every $i \in \{1, \dots, n\}$, there exists a non-zero element $e_i \in \mathrm{Hom}_{\mathbb{Q}}(A_i, B)$. By (3.7) the element e_i corresponds to a non-zero homomorphism $\eta_i \colon (A_i)_K \to E$. Composing η_i with homomorphisms $B_K \to (A_i)_K$ and $E \to B_K$, we get a non-zero endomorphism η_i' of B defined over K. Since all endomorphisms of B are defined over L, η_i' itself is defined over $K_0 \coloneqq K \cap L$. Let $E_i \coloneqq \eta_i'((A_i)_{K_0})$. This is an elliptic curve over K_0 with the property that $(E_i)_K \simeq E$. Let $G_0 \coloneqq \mathrm{Gal}(K_0/\mathbb{Q})$. Since E_i is a factor of $(A_i)_{K_0}$ and A_i an abelian variety over $\mathbb{Q}$, also ${}^{\sigma}E_i$ is a factor of $(A_i)_{K_0}$ for every $\sigma \in G_0$. Let $C_i \coloneqq \sum_{\sigma \in G_0} {}^{\sigma}E_i$. This is an abelian subvariety of $(A_i)_{K_0}$, but it is also defined over $\mathbb{Q}$. Hence, it is a subvariety of A_i. But A_i is simple, and therefore $C_i \sim A_i$. This proves that $(A_i)_{K_0}$ is isogenous to a product of conjugates of E_i.

Next, we claim that E_i is completely defined over K_0. Let $B_0 \coloneqq \mathrm{Res}_{K/K_0}(E) \simeq \mathrm{Res}_{K/K_0}((E_i)_K)$. Again, it is easy to see using the definition of restriction of scalars, that E_i is a factor of B_0. Fix a non-trivial map $B_0 \to E_i$ and let $E_i^{(K/K_0)}$ be the abelian variety fitting in the exact sequence

$$0 \to E_i^{(K/K_0)} \to B_0 \to E_i \to 0.$$

The notation is motivated by the fact that if $K/K_0 = K_0(\sqrt{d})$ for some non-square $d \in K_0$, then $E_i^{(K/K_0)}$ is the quadratic twist of E_i by d. Thus,

$$B = \mathrm{Res}_{K/\mathbb{Q}}(E) \simeq \mathrm{Res}_{K_0/\mathbb{Q}}(B_0) \sim \mathrm{Res}_{K_0/\mathbb{Q}}(E_i) \times \mathrm{Res}_{K_0/\mathbb{Q}}(E_i^{(K/K_0)}).$$

By assumption, B is of GL_2-type. Hence, by Lemma 1.3.2 all its factors over $\mathbb{Q}$ are of GL_2-type. This implies, in particular, that $\mathrm{Res}_{K_0/\mathbb{Q}}(E_i)$ is of GL_2-type. Therefore E_i is strongly modular over K_0 and since $K_0/\mathbb{Q}$ is abelian, by Theorem 3.2.1 E_i is completely defined over K_0.

This shows that all endomorphisms of A_i are defined over K_0, and therefore $L_i \subseteq K_0$. Since i was arbitrary, it follows that $L \subseteq K_0$ and consequently $L = K_0 \subseteq K$. Thus, $B_K \sim (E_0)_K^{[K:\mathbb{Q}]}$ for some $\mathbb{Q}$-curve E_0 completely defined over L.

Step 2. Let $\widetilde{K}$ be the Galois closure of K, let $G \coloneqq \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$, let $H \coloneqq \mathrm{Gal}(\widetilde{K}/K)$ and let $H_L \coloneqq \mathrm{Gal}(\widetilde{K}/L)$. To show that K is Galois, we will prove the following claim:

$$\dim \mathrm{End}^0_{\mathbb{Q}}(B) = |H \backslash G / H|.$$

Here $H\backslash G/H$ denotes the set of orbits of the left cosets of H in G under the left action given by multiplication by H. This set has cardinality at most $[G : H]$, with equality precisely when H is normal in G. Since B is of GL_2-type, $\mathrm{End}^0_{\mathbb{Q}}(B)$ has to contain a number field of degree equal to $\dim B = [G : H]$. The proof of the proposition follows then immediately.

Let $\widetilde{B} \coloneqq \mathrm{Res}_{\widetilde{K}/\mathbb{Q}}(E_{\widetilde{K}})$. Using the fact that $\mathrm{Res}_{\widetilde{K}/\mathbb{Q}}(E_{\widetilde{K}}) = \mathrm{Res}_{K/\mathbb{Q}}(\mathrm{Res}_{\widetilde{K}/K}(E_{\widetilde{K}}))$ and the universal property defining the restriction of scalars, one checks that B is a factor of $\widetilde{B}$. Hence there is a homomorphism $\pi \colon \widetilde{B} \to B$ giving rise to a split exact sequence of abelian varieties up to isogeny

$$0 \to C \to \widetilde{B} \to B \to 0,$$

where $C \coloneqq (\ker \pi)_0$ is the connected component of $\ker \pi$ containing the identity. Let

$$\mathcal{R} = \{\varphi \in \mathrm{End}_{\mathbb{Q}}(\widetilde{B}) \colon \varphi(C) \subseteq C\}.$$

There is a homomorphism

$$\Phi\colon \mathcal{R}\otimes\mathbb{Q}\to \mathrm{End}^0_{\mathbb{Q}}(B)$$

$$\varphi\otimes q\mapsto \overline{\varphi}\otimes q$$

where $\overline{\varphi}$ is the unique endomorphism which makes the following diagram commute:

$$\begin{array}{ccc} \widetilde{B} & \xrightarrow{\varphi} & \widetilde{B} \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ B & \xrightarrow{\overline{\varphi}} & B. \end{array}$$

Notice that Φ is surjective, since every endomorphism of B can be extended to an endomorphism of $\widetilde{B}$ via the isogeny $\widetilde{B}\sim B\times C$. Moreover,

$$\ker\Phi \coloneqq \{\varphi\in\mathcal{R}\colon \varphi(B)\subseteq C\}.$$

To prove our claim, we will compute the codimension of $\mathrm{End}^0_{\mathbb{Q}}(B)$ in $\mathrm{End}^0_{\mathbb{Q}}(\widetilde{B})$. Both these algebras are in particular $\mathbb{Q}$-vector spaces of finite dimension, so we will consider a generic vector $v\in\mathrm{End}^0_{\mathbb{Q}}(\widetilde{B})$ and determine the linear system of equations describing the condition $v\in\ker\Phi$.

The homomorphism

$$G\to G/H_L$$

$$\tau\mapsto\overline{\tau}$$

factors through the projection

$$G\to G/H$$

$$\tau\mapsto \tau H.$$

By what we proved in Step 1, there exists an elliptic curve E_0, completely defined over L, such that $E=(E_0)_K$. We have decompositions

$$\begin{aligned} \widetilde{B}_{\widetilde{K}} &\simeq \prod_{\tau\in G} ({}^{\overline{\tau}}E_0)_{\widetilde{K}} \\ B_{\widetilde{K}} &\simeq \prod_{x\in G/H} ({}^{\overline{x}}E_0)_{\widetilde{K}}. \end{aligned} \tag{3.8}$$

The full endomorphism ring of $\widetilde{B}_{\widetilde{K}}$ is given by $\prod_{\tau,\tau'\in G}\mathrm{Hom}(({}^{\overline{\tau}}E_0)_{\widetilde{K}},({}^{\overline{\tau'}}E_0)_{\widetilde{K}})$. By (3.7) we have that

$$\begin{aligned} \mathrm{End}_{\mathbb{Q}}(\widetilde{B}) &\simeq \prod_{\tau\in G}\mathrm{Hom}\left(({}^{\overline{\tau}}E_0)_{\widetilde{K}},(E_0)_{\widetilde{K}}\right) = \\ &= \left\{\left(\varphi_\tau\in\mathrm{Hom}\left(({}^{\overline{\tau}}E_0)_{\widetilde{K}},(E_0)_{\widetilde{K}}\right)\right)_{\tau\in G}\right\}. \end{aligned} \tag{3.9}$$

Thus, $\dim\mathrm{End}^0_{\mathbb{Q}}(\widetilde{B})=|G|=\dim\widetilde{B}$. Notice that $\mathrm{End}_{\mathbb{Q}}(\widetilde{B})$ is isomorphic to the subset of $\mathrm{End}_{\widetilde{K}}(\widetilde{B})$ given by $\{(\varphi_{\tau,\tau'})_{\tau,\tau'\in G}\colon \forall\,\sigma\in G, {}^{\sigma}\varphi_{\tau,\tau'}=\varphi_{\rho\tau,\rho\tau'}\}$ via the map that sends $(\varphi_\tau)_{\tau\in G}\mapsto({}^{\tau'}\varphi_{\tau'^{-1}\tau,1})_{\tau,\tau'}$.

The projection $\pi\colon \widetilde{B} \to B$ induces, under identifications (3.8), a map

$$\begin{aligned} \pi_{\widetilde{K}}\colon \widetilde{B}_{\widetilde{K}} &\to B_{\widetilde{K}} \\ (P_\tau)_{\tau\in G} &\mapsto \left(\sum_{\tau\colon \tau H = x} P_\tau \right)_{x\in G/H}. \end{aligned}$$

Therefore the kernel of $\pi_{\widetilde{K}}$ is given by:

$$\begin{aligned} \ker \pi_{\widetilde{K}} &= \left\{ (P_\tau)_{\tau\in G} \in \widetilde{B}_{\widetilde{K}} \colon \forall\, \sigma \in G\colon \sum_{\tau\in G\colon \tau H = \sigma H} P_\tau = 0 \right\} = \\ &= \left\{ (P_\tau)_{\tau\in G}\colon\ \forall\, \sigma \in G/H\colon \sum_{\rho\in H} P_{\sigma\rho} = 0 \right\}. \end{aligned} \tag{3.10}$$

Now for every $\sigma \in G/H$ and every $\rho \in H \setminus \{\mathrm{id}\}$, let $P \in \left({}^{\overline{\sigma}}E_0\right)_{\widetilde{K}}$. Define $Q_{\sigma,\rho}(P) = (P_\tau)_{\tau\in G}$ where

$$P_\tau = \begin{cases} P & \text{if } \tau = \sigma \\ -P & \text{if } \tau = \sigma\rho \\ 0 & \text{otherwise.} \end{cases}$$

It is easy to check using the description given in (3.10) that the collection of all $Q_{\sigma,\rho}(P)$ constructed in this way generates $\ker \pi_{\widetilde{K}}$. Given any $Q_{\sigma,\rho}(P)$ and any $(\varphi_{\tau,\tau'})_{\tau,\tau'} \in \mathrm{End}(\widetilde{B})$, we have that:

$$\varphi(Q_{\sigma,\rho}(P)) = (\varphi_{\sigma,\tau'}(P) - \varphi_{\sigma\rho,\tau'}(P))_{\tau'\in G}.$$

Thus the image of $\varphi(Q_{\sigma,\rho}(P))$ in $B_{\widetilde{K}}$ via $\pi_{\widetilde{K}}$ is given by:

$$\left(\sum_{\tau\in G\colon \tau H = x} (\varphi_{\sigma,\tau}(P) - \varphi_{\sigma\rho,\tau}(P)) \right)_{x\in G/H}.$$

Recall that $\varphi_{\sigma,\tau} = {}^{\tau}\varphi_{\tau^{-1}\sigma,1}$ and this corresponds to ${}^{\tau}\varphi_{\tau^{-1}\sigma}$ in the description given in (3.9). Thus,

$$\pi_{\widetilde{K}}(\varphi(Q_{\sigma,\rho}(P))) = \left(\sum_{\tau\in G\colon \tau H = \beta H} {}^{\tau}(\varphi_{\tau^{-1}\sigma}({}^{\tau^{-1}}P) - \varphi_{\tau^{-1}\sigma\rho}({}^{\tau^{-1}}P)) \right)_{\beta\in G/H}. \tag{3.11}$$

Now write $\tau = \beta\alpha$, with $\alpha \in H$. Then we can rewrite (3.11) as

$$\left(\sum_{\alpha\in H} {}^{\beta\alpha}(\varphi_{\alpha^{-1}\beta^{-1}\sigma} - \varphi_{\alpha^{-1}\beta^{-1}\sigma\rho})({}^{\alpha^{-1}\beta^{-1}}P) \right)_{\beta\in G/H}.$$

Since P was arbitrary, it follows that $\mathcal{R}$ coincides with the set of endomorphisms $(\varphi_\tau)_{\tau\in G} \in \mathrm{End}_{\mathbb{Q}}(\widetilde{B})$ such that

$$\sum_{\alpha\in H} {}^{\alpha}(\varphi_{\alpha^{-1}\beta^{-1}\sigma} - \varphi_{\alpha^{-1}\beta^{-1}\sigma\rho}) = 0, \quad \forall\, \sigma,\beta \in G/H, \quad \forall \rho \in H \setminus \{1\}.$$

It is clear that for fixed σ, ρ, changing β to $h\beta$ for any $h \in H$ does not change the sum above. Thus, recalling that all endomorphisms of B are defined over K, our condition becomes

$$\sum_{\alpha \in H} (\varphi_{\alpha\gamma} - \varphi_{\alpha\gamma\rho}) = 0, \quad \forall\, \gamma \in H\backslash G/H, \quad \forall\, \rho \in H. \tag{3.12}$$

It is clear that whenever $\rho = \sigma\rho'$, where $\sigma, \rho' \in H$ and $\sigma \in \mathrm{Stab}_H(H\gamma)$, then $\sum_{\alpha \in H} \varphi_{\alpha\gamma\rho} = \sum_{\alpha \in H} \varphi_{\alpha\gamma\rho'}$. Here $\mathrm{Stab}_H(H\gamma)$ is the stabilizer of $H\gamma \in H\backslash G$ under the action of H on $H\backslash G$ given by right multiplication by H. On the other hand, one can view $H\gamma H$ as the set of right orbits of $H\gamma$ under right multiplication by H. In this setting, there is a bijection

$$\mathrm{Stab}_H(H\gamma)\backslash H \to H\backslash H\gamma H$$

$$\rho \mapsto H\gamma\rho.$$

Thus, we can rewrite (3.12) as

$$\sum_{\alpha \in H} (\varphi_{\alpha\gamma} - \varphi_{\alpha x}) = 0, \quad \forall\, \gamma \in H\backslash G/H, \quad \forall\, x \in H\backslash G.$$

It is easy to see that this is equivalent to:

$$\forall\, x, y \in H\backslash G\colon xH = yH \Longrightarrow \sum_{\alpha \in x} \varphi_\alpha = \sum_{\beta \in y} \varphi_\beta. \tag{3.13}$$

A small computation shows that condition (3.13) gives a system of $[G : H] - |H\backslash G/H|$ independent equations defining $\mathcal{R}$. This shows that the codimension of $\mathcal{R} \otimes \mathbb{Q}$ inside $\mathrm{End}^0_{\mathbb{Q}}(\widetilde{B})$ is exactly $[G : H] - |H\backslash G/H|$.

To determine the codimension of $\ker \Phi$ inside $\mathrm{End}_{\mathbb{Q}}(\widetilde{B})$, one can carry out similar computations, but this time the points $Q_{\sigma,\rho}(P) = (P_\tau)_{\tau \in G}$ will simply be defined by:

$$P_\tau = \begin{cases} P & \text{if } \tau = \sigma \\ 0 & \text{otherwise.} \end{cases}$$

Thus, we get that $(\varphi_\tau)_{\tau \in G} \in \ker \Phi$ if and only if for every $x \in H\backslash G$ we have $\sum_{\alpha \in x} \varphi_\alpha = 0$. This defines a subspace of $\mathrm{End}^0_{\mathbb{Q}}(\widetilde{B})$ of codimension $[G : H]$. Thus, the codimension of $\ker \Phi$ inside $\mathcal{R}$ is $|H\backslash G/H|$, and the claim is proven. □

The second preliminary result shows that the 2-torsion of the Brauer group of $\mathbb{Q}$ is generated by cocycles inflated from certain symmetric ones.

Proposition 3.6.5. The inflation map $\mathrm{Inf}\colon H^2_s(G^{\mathrm{ab}}_{\mathbb{Q}}, \{\pm 1\}) \to \mathrm{Br}(\mathbb{Q})[2]$ is an isomorphism.

Proof. Consider the exact sequence

$$1 \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}) \to G_{\mathbb{Q}} \to G^{\mathrm{ab}}_{\mathbb{Q}} \to 1.$$

By inflation-restriction applied to $\{\pm 1\}$ and $\overline{\mathbb{Q}}^*$ (with the natural Galois action) we get two exact sequences which fit into a commutative diagram

$$\begin{array}{ccccc} H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}),\{\pm1\})^{G_{\mathbb{Q}}^{\mathrm{ab}}} & \xrightarrow{\mathrm{trg}} & H^2(G_{\mathbb{Q}}^{\mathrm{ab}},\{\pm1\}) & \xrightarrow{\mathrm{Inf}} & \mathrm{Br}(\mathbb{Q})[2] \\ \downarrow & & \downarrow{\scriptstyle \varphi_{\mathbb{Q}^{\mathrm{ab}}}} & & \downarrow \\ H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}),\overline{\mathbb{Q}}^*)^{G_{\mathbb{Q}}^{\mathrm{ab}}} & \xrightarrow{\mathrm{trg}} & H^2(G_{\mathbb{Q}}^{\mathrm{ab}},\mathbb{Q}^{\mathrm{ab}*}) & \xrightarrow{\mathrm{Inf}} & \mathrm{Br}(\mathbb{Q}). \end{array}$$

By Hilbert's theorem 90, $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}),\overline{\mathbb{Q}}^*)$ is trivial, so the map $\mathrm{Inf}\colon H^2(G_{\mathbb{Q}}^{\mathrm{ab}},\mathbb{Q}^{\mathrm{ab}*}) \to \mathrm{Br}(\mathbb{Q})$ is injective. On the other hand, also the map $\mathrm{Br}(\mathbb{Q})[2] \to \mathrm{Br}(\mathbb{Q})$ is injective, and this shows that $\ker\varphi_{\mathbb{Q}^{\mathrm{ab}}}$ coincides with the kernel of $\mathrm{Inf}\colon H^2(G_{\mathbb{Q}}^{\mathrm{ab}},\{\pm1\}) \to \mathrm{Br}(\mathbb{Q})[2]$. By Lemma 3.5.7 we have that $H^2_s(G_{\mathbb{Q}}^{\mathrm{ab}},\{\pm1\}) \cap \ker\varphi_{\mathbb{Q}^{\mathrm{ab}}} = \{1\}$, since a non-trivial element in this intersection would correspond to a non-trivial extension of $\mathbb{Q}^{\mathrm{ab}}$ which is Galois and abelian over $\mathbb{Q}$. Therefore the map $\mathrm{Inf}\colon H^2_s(G_{\mathbb{Q}}^{\mathrm{ab}},\{\pm1\}) \to \mathrm{Br}(\mathbb{Q})[2]$ is injective.

To prove surjectivity, we first claim that

$$H^2_s(G_{\mathbb{Q}}^{\mathrm{ab}},\{\pm1\}) \simeq H^2_s(\widehat{\mathbb{Z}}^*,\{\pm1\}) \simeq \bigoplus_p H^2_s(\mathbb{Z}_p^*,\{\pm1\}). \tag{3.14}$$

For every prime p, we denote by $\mathbb{Q}(\zeta_{p^\infty})$ the field obtained by adjoining to $\mathbb{Q}$ all roots of unity of p-power order. Recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^*$. The exact sequence

$$1 \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}(\zeta_{p^\infty})) \to G_{\mathbb{Q}}^{\mathrm{ab}} \to \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \to 1 \tag{3.15}$$

splits. Thus in the inflation-restriction exact sequence

$$1 \to H^1(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q},\{\pm1\}) \to H^1(G_{\mathbb{Q}}^{\mathrm{ab}},\{\pm1\}) \to H^1(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}(\zeta_{p^\infty}),\{\pm1\}) \to$$

$$\xrightarrow{\mathrm{trg}} H^2(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q},\{\pm1\}) \to H^2(G_{\mathbb{Q}}^{\mathrm{ab}},\{\pm1\}),$$

the map trg is zero. This shows that that the inflation map $\mathrm{Inf}\colon H^2(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q},\{\pm1\}) \to H^2(G_{\mathbb{Q}}^{\mathrm{ab}},\{\pm1\})$ is injective, and therefore it restricts to an injection

$$\mathrm{Inf}_p\colon H^2_s(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q},\{\pm1\}) \hookrightarrow H^2_s(G_{\mathbb{Q}}^{\mathrm{ab}},\{\pm1\}).$$

If l is a prime different from p, then

$$\mathrm{Inf}_p(H^2_s(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q},\{\pm1\})) \cap \mathrm{Inf}_l(H^2_s(\mathbb{Q}(\zeta_{l^\infty})/\mathbb{Q},\{\pm1\})) = \{1\}.$$

In fact, let c be an element in the intersection and notice that there is a split exact sequence

$$1 \to \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})\mathbb{Q}(\zeta_{l^\infty})/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_{l^\infty})) \to 1$$

which induces an isomorphism

$$H^2_s(\mathbb{Q}(\zeta_{p^\infty})\mathbb{Q}(\zeta_{l^\infty})/\mathbb{Q},\{\pm1\}) \simeq H^2_s(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q},\{\pm1\}) \times H^2_s(\mathbb{Q}(\zeta_{l^\infty})/\mathbb{Q},\{\pm1\}).$$

This shows that c is trivial in $H^2_s(\mathbb{Q}(\zeta_{p^\infty})\mathbb{Q}(\zeta_{l^\infty})/\mathbb{Q},\{\pm1\})$. Then use the fact that the map Inf_p factors via

$$\mathrm{Inf}^p_{pl}\colon H^2_s(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q},\{\pm1\}) \to H^2_s(\mathbb{Q}(\zeta_{p^\infty})\mathbb{Q}(\zeta_{l^\infty})/\mathbb{Q},\{\pm1\})$$

followed by

$$\mathrm{Inf}^{pl}_{\mathbb{Q}^{\mathrm{ab}}}\colon H^2_s(\mathbb{Q}(\zeta_{p^\infty})\mathbb{Q}(\zeta_{l^\infty})/\mathbb{Q},\{\pm 1\}) \to H^2_s(G^{\mathrm{ab}}_{\mathbb{Q}},\{\pm 1\})$$

to conclude that c is trivial in $H^2_s(G^{\mathrm{ab}}_{\mathbb{Q}},\{\pm 1\})$.

Thus, we have an injective map

$$\bigoplus_p \mathrm{Inf}_p\colon \bigoplus_p H^2_s(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q},\{\pm 1\}) \to H^2_s(G^{\mathrm{ab}}_{\mathbb{Q}},\{\pm 1\}).$$

To see that it is also surjective, we use the fact that any class $c \in H^2_s(G^{\mathrm{ab}}_{\mathbb{Q}},\{\pm 1\})$ factors through $\mathbb{Q}(\zeta_N)$ for some $N \in \mathbb{N}$. If $p_1,\dots,p_r$ are the distinct primes dividing N, then $\mathbb{Q}(\zeta_N) \subseteq K_N \coloneqq \prod_{i=1}^{r} \mathbb{Q}(\zeta_{p_i^\infty})$ and we can think of c as the inflation of an element of $H^2_s(K_N,\{\pm 1\}) = \bigoplus_{i=1}^{r} H^2_s(\mathbb{Q}(\zeta_{p_i^\infty}),\{\pm 1\})$. This concludes the proof of claim (3.14).

To compute $H^2_s(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q},\{\pm 1\}) \simeq H^2_s(\mathbb{Z}_p^*,\{\pm 1\})$, recall that

$$\mathbb{Z}_p^* \simeq \begin{cases} (\mathbb{Z}/4\mathbb{Z})^* \times \mathbb{Z}_2 & \text{if } p = 2 \\ \mathbb{F}_p^* \times \mathbb{Z}_p & \text{if } p > 2 \end{cases}.$$

Thus we have that

$$H^2_s(\mathbb{Z}_p^*,\{\pm 1\}) \simeq \begin{cases} H^2_s((\mathbb{Z}/4\mathbb{Z})^*,\{\pm 1\}) \times H^2_s(\mathbb{Z}_2,\{\pm 1\}) & \text{if } p = 2 \\ H^2_s(\mathbb{F}_p^*,\{\pm 1\}) \times H^2_s(\mathbb{Z}_p,\{\pm 1\}) & \text{if } p > 2 \end{cases}.$$

Now we claim that $H^2(\mathbb{Z}_p,\{\pm 1\}) = H^2_s(\mathbb{Z}_p,\{\pm 1\}) = \{1\}$ for all p. If $p > 2$ this follows easily from the fact that $\mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ and $H^2(\mathbb{Z}/p^n\mathbb{Z},\{\pm 1\}) = \{1\}$ for all $n \in \mathbb{N}$. For $p = 2$, note that for all $n \in \mathbb{N}$ we have that $H^1(\mathbb{Z}/2^n\mathbb{Z},\{\pm 1\}) \simeq H^2(\mathbb{Z}/2^n\mathbb{Z},\{\pm 1\}) \simeq \{\pm 1\}$. Therefore if $n < m$, considering the exact sequence

$$0 \to \mathbb{Z}/2^{m-n}\mathbb{Z} \to \mathbb{Z}/2^m\mathbb{Z} \to \mathbb{Z}/2^n\mathbb{Z} \to 0$$

and applying inflation-restriction to get the exact sequence

$$1 \to H^1(\mathbb{Z}/2^n\mathbb{Z},\{\pm 1\}) \to H^1(\mathbb{Z}/2^m\mathbb{Z},\{\pm 1\}) \to H^1(\mathbb{Z}/2^{m-n}\mathbb{Z},\{\pm 1\}) \to$$

$$\overset{\mathrm{trg}}{\to} H^2(\mathbb{Z}/2^n\mathbb{Z},\{\pm 1\}) \overset{\mathrm{Inf}}{\to} H^2(\mathbb{Z}/2^m\mathbb{Z},\{\pm 1\}),$$

we get that trg is an isomorphism. This shows that $\mathrm{Inf}\colon H^2(\mathbb{Z}/2^n\mathbb{Z},\{\pm 1\}) \to H^2(\mathbb{Z}/2^m\mathbb{Z},\{\pm 1\})$ is the zero map; it follows immediately that

$$H^2(\mathbb{Z}_2,\{\pm 1\}) \simeq \varinjlim_{n\in\mathbb{N}} H^2(\mathbb{Z}/2^n\mathbb{Z},\{\pm 1\}) = \{1\}.$$

Since for every prime $p > 2$ we have that $H^2(\mathbb{F}_p^*,\{\pm 1\}) \simeq H^2((\mathbb{Z}/4\mathbb{Z})^*,\{\pm 1\}) \simeq \{\pm 1\}$, we finally get that

$$H^2_s(G^{\mathrm{ab}}_{\mathbb{Q}},\{\pm 1\}) \simeq \bigoplus_{p \text{ prime}} \{\pm 1\}.$$

To conclude the proof, let l be a prime and consider the element $\varepsilon_l = (t_p)_p \in H^2_s(G^{\mathrm{ab}}_{\mathbb{Q}}, \{\pm 1\})$ defined by:

$$t_p = \begin{cases} -1 & \text{if } p = l \\ 1 & \text{otherwise.} \end{cases}$$

Notice that we proved above that ε_l is the inflation to $G^{\mathrm{ab}}_{\mathbb{Q}}$ of the unique non-trivial element in $H^2(\mathbb{Q}(\zeta_{l^\infty})/\mathbb{Q}, \{\pm 1\})$. We will show that $\mathrm{Inf}(\varepsilon_l) \in \mathrm{Br}(\mathbb{Q})[2]$ corresponds to the quaternion algebra ramified at l and ∞. This implies in particular that $\mathrm{Inf}\colon H^2_s(G^{\mathrm{ab}}_{\mathbb{Q}}, \{\pm 1\}) \to \mathrm{Br}(\mathbb{Q})[2]$ is surjective, which is what we wanted to prove.

To compute $\mathrm{Inf}(\varepsilon_l) \in \mathrm{Br}(\mathbb{Q})[2]$, we look at the local components. Recall that for every place v of $\mathbb{Q}$ there is an isomorphism $\mathrm{Br}(\mathbb{Q}_v) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ and that there exists an exact sequence

$$0 \longrightarrow \mathrm{Br}(\mathbb{Q}) \longrightarrow \bigoplus\nolimits_v \mathrm{Br}(\mathbb{Q}_v) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0\,,$$

where v runs over all places of $\mathbb{Q}$; the first non-trivial map is the product of all the restriction maps $\mathrm{Res}_v\colon \mathrm{Br}(\mathbb{Q}) \to \mathrm{Br}(\mathbb{Q}_v)$ and the second one is the sum of the components.

Let v be a finite place of $\mathbb{Q}$ different from l. We claim that $\mathrm{Res}_v(\mathrm{Inf}(\varepsilon_l)) = 0$ in $\mathrm{Br}(\mathbb{Q}_v)$. This implies that $\mathrm{Inf}(\varepsilon_l) \in \mathrm{Br}(\mathbb{Q})[2]$ is ramified precisely at l and ∞, because ε_l is non-trivial in $H^2_s(G^{\mathrm{ab}}_{\mathbb{Q}}, \{\pm 1\})$ and the map $\mathrm{Inf}\colon H^2_s(G^{\mathrm{ab}}_{\mathbb{Q}}, \{\pm 1\}) \to \mathrm{Br}(\mathbb{Q})[2]$ is injective, as we already proved.

Note that $\mathrm{Res}_v(\mathrm{Inf}(\varepsilon_l))$ is the inflation to $\mathrm{Br}(\mathbb{Q}_v)$ of the unique non-trivial element ε_l^{nr} in $H^2_s(\mathbb{Q}_v(\zeta_{l^\infty})/\mathbb{Q}_v, \{\pm 1\})$. Let $\mathbb{Q}_v^{nr}$ be the maximal unramified extension of $\mathbb{Q}_v$. Since $\mathbb{Q}_v(\zeta_{l^\infty})$ is an unramified extension of $\mathbb{Q}_v$, we can consider ε_l^{nr} as an element of $\mathrm{Br}(\mathbb{Q}_v^{nr})$. By [65, Theorem XII.1], $\mathrm{Br}(\mathbb{Q}_v^{nr}) \xrightarrow{\sim} \mathrm{Br}(\mathbb{Q}_v)$, via inflation. Now the isomorphism $\mathrm{Br}(\mathbb{Q}_v) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ is constructed in the following way: the exact sequence

$$1 \to \mathcal{O}^*_{\mathbb{Q}_v^{nr}} \to \mathbb{Q}_v^{nr\,*} \xrightarrow{v} \mathbb{Z} \to 0,$$

where v is the valuation map, yields a (split) exact sequence

$$0 \to \mathrm{Br}(\mathbb{F}_v) \to \mathrm{Br}(\mathbb{Q}_v) \to H^2(\mathbb{Q}_v^{nr}/\mathbb{Q}_v, \mathbb{Z}) \to 0$$

(see [65, §XII.3]); as the Brauer group of a finite field is trivial (see [65, §X.7]), we get an isomorphism, induced from the valuation map, $v\colon \mathrm{Br}(\mathbb{Q}_v^{nr}) \to H^2(\mathbb{Q}_v^{nr}/\mathbb{Q}_v, \mathbb{Z})$. The long exact sequence in cohomology induced by the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, together with the fact that $\mathbb{Q}$ is cohomologically trivial, gives the desired isomorphism $\mathbb{Q}/\mathbb{Z} \simeq H^1(\mathbb{Q}_v^{nr}/\mathbb{Q}_v, \mathbb{Q}/\mathbb{Z}) \to H^2(\mathbb{Q}_v^{nr}/\mathbb{Q}_v, \mathbb{Z})$. Now the claim is easily proven by the fact that $v(\varepsilon_l^{nr}) = 0$ in $\mathbb{Q}/\mathbb{Z} \simeq \mathrm{Br}(\mathbb{Q}_v)$. □

Proof of Theorem 3.6.2. First suppose that E is $\overline{\mathbb{Q}}$-isomorphic to a strongly modular curve E' over a number field M. By Proposition 3.6.4, M is Galois over $\mathbb{Q}$ and by Theorem 3.2.1, M is abelian. Thus, K is abelian over $\mathbb{Q}$. Since E_M is $\overline{\mathbb{Q}}$-isomorphic to E', the latter is a quadratic twist of E_M. Let $\alpha \in \overline{\mathbb{Q}}$ be such that $\alpha^2 \in M$ and such that $E_M^{(\alpha)}$ is isomorphic to E' over M. By Theorem 3.2.1, E' is completely defined over M, so $E'_{M(\alpha)}$ is completely defined over $M(\alpha)$. Since $E_{M(\alpha)} \simeq (E^{(\alpha)})_{M(\alpha)} \simeq E'_{M(\alpha)}$, it follows that $E_{M(\alpha)}$ is completely defined over $M(\alpha)$. Let L be the minimal field of definition of E, so that $L \subseteq M(\alpha)$. If $L \subseteq M$, then L is abelian over $\mathbb{Q}$. Otherwise, namely if

$L \subsetneq M$, then LM is a non-trivial extension of M, so it has to coincide with $M(\alpha)$. This shows that $M(\alpha)$ is Galois over $\mathbb{Q}$. Since $E'^{(\alpha)} \simeq E_M^{(\alpha^2)} \simeq E_M$, by Lemma 3.2.2 it follows that E_M is completely defined over M, which proves that $L \subseteq M$, contradiction. Hence, L is abelian over $\mathbb{Q}$.

Let us now prove the converse, so assume that the minimal field of definition L is abelian over $\mathbb{Q}$. Let $\xi_L = \xi_L(E) \in Z^2(L/\mathbb{Q}, \mathbb{Q}^*)$ be the 2-cocycle attached to E. For every extension F/L which is Galois over $\mathbb{Q}$, we denote by $[\xi_F]$ the inflation of $[\xi_L]$ to $H^2(F/\mathbb{Q}, \mathbb{Q}^*)$. As usual, the sign component of $[\xi_F]$ will be denoted by $[\xi_F^{\pm}]$. Let $M/\mathbb{Q}$ be an abelian extension containing L. By Theorem 3.2.1, Lemma 3.2.2 and Remark 3.2.3 we know that E_M has a strongly modular quadratic twist completely defined over M if and only if there exists $\lambda \in M^* \setminus (M^*)^2$ such that:

a) $M(\sqrt{\lambda})$ is Galois over $\mathbb{Q}$;

b) if $c \in H^2(M/\mathbb{Q}, \{\pm 1\})$ is the cohomology class attached to the exact sequence:

$$1 \to \{\pm 1\} \to \mathrm{Gal}(M(\sqrt{\lambda})/\mathbb{Q}) \to \mathrm{Gal}(M/\mathbb{Q}) \to 1$$

then $[\xi_M^{\pm}] \cdot c \in H_s^2(M/\mathbb{Q}, \{\pm 1\})$

Let $\varphi_M \colon H^2(M/\mathbb{Q}, \{\pm 1\}) \to H^2(M/\mathbb{Q}, M^*)$ be the canonical map induced by the inclusion $\{\pm 1\} \subseteq M^*$. By Lemma 3.5.7, conditions a) and b) are satisfied if and only if there exists $c \in \ker \varphi_M$ such that $[\xi_M^{\pm}] \cdot c \in H_s^2(M/\mathbb{Q}, \{\pm 1\})$. Assume that this is the case. The following diagram commutes

$$\begin{array}{ccc} H^2(M/\mathbb{Q}, \{\pm 1\}) & \xrightarrow{\varphi_M} & H^2(M/\mathbb{Q}, M^*) \\ \Big\downarrow{\scriptstyle \mathrm{Inf}} & & \Big\downarrow \\ H^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\}) & \xrightarrow{\varphi_{\mathbb{Q}^{\mathrm{ab}}}} & H^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \mathbb{Q}^{\mathrm{ab}*}) \end{array}$$

(here the map on the right is the composition of the inflation map $H^2(M/\mathbb{Q}, M^*) \to H^2(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}, M^*)$ with the natural map $H^2(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}, M^*) \to H^2(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}, \mathbb{Q}^{\mathrm{ab}*})$) and therefore we see that there exists $c \in \ker \varphi_{\mathbb{Q}^{\mathrm{ab}}}$ such that $\xi_{\mathbb{Q}^{\mathrm{ab}}}^{\pm} \cdot c \in H_s^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\})$.

Conversely, if such a cohomology class exists then it factors through some finite abelian extension $M/\mathbb{Q}$, which we can assume to contain L, and therefore there exists $c \in \ker \varphi_M$ such that $[\xi_M^{\pm}] \cdot c \in H_s^2(M/\mathbb{Q}, \{\pm 1\})$. This shows that there exists an abelian number field M and a $\lambda \in M^* \setminus (M^*)^2$ which respect conditions a) and b) if and only if there exists a class $c \in H^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \pm 1)$ such that $c \in \ker \varphi_{\mathbb{Q}^{\mathrm{ab}}}$ and $[\xi_{\mathbb{Q}^{\mathrm{ab}}}^{\pm}] \cdot c \in H_s^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\})$.

As noticed in the proof of Proposition 3.6.5, $\ker \varphi_{\mathbb{Q}^{\mathrm{ab}}}$ coincides with the kernel of $\mathrm{Inf} \colon H^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\}) \to \mathrm{Br}(\mathbb{Q})[2]$. Therefore, it remains to prove the following claim: there exists $c \in \ker(\mathrm{Inf} \colon H^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\}) \to \mathrm{Br}(\mathbb{Q})[2])$ such that $[\xi_{\mathbb{Q}^{\mathrm{ab}}}^{\pm}] \cdot c \in H_s^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\})$. This amounts to saying that the image of $[\xi_{\mathbb{Q}^{\mathrm{ab}}}^{\pm}]$ in $\mathrm{Br}(\mathbb{Q})[2]$ belongs to the image of $H_s^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\})$. By Proposition 3.6.5, this is always the case, and the proof is complete. □

Chapter 4

On the Mertens–Cesàro theorem for number fields

This chapter is a paper, written in collaboration with Dr. G. Micheli, which is to appear in the Bulletin of the Australian Mathematical Society.

4.1 Introduction

In 1874 Mertens proved that the natural density of the set of coprime pairs of rational integers is $1/\zeta(2)$, where ζ is the Riemann zeta function [51]. In 1881 Cesàro independently asked the same question in [13] and provided the solution two years later in [14], getting the same result as Mertens. Another proof of this result is presented in the book by Hardy and Wright [36, Theorem 330], while a generalization to the case of m-tuples of integers has been more recently given in [57].

If one tries to extend the formulation of the theorem to the case of algebraic integers, one encounters some obstructions from the very beginning. In the next paragraphs the reader can find some of the motivations that led to our approach to the problem, especially concerning the definition of the density for a subset of the ring of algebraic integers $\mathcal{O}$ of a number field K.

Indeed, for the case of $\mathbb{Z}$, there exists a "canonical" way to compute the density of a set $A \subseteq \mathbb{Z}$: this can be in fact defined as the limit in B (if it exists) of the sequence $|A \cap [-B, B[|/(2B)$. This definition extends to the density of a set $A \subseteq \mathbb{Z}^m$ by considering the limit of the sequence $|A \cap [-B, B[^m|/(2B)^m$ as B goes to infinity. This definition characterizes the probability that, given the m-dimensional hypercube of large side B centered in the origin, a uniformly random selected integer point has all relatively prime entries.

What can actually be done in the setting of algebraic integers is to consider the analogous problem for the set of m-tuples of ideals of $\mathcal{O}$ using a suitable definition of density involving the norm function. Very interesting results in this direction can be found in [73]. On the other hand, if we want a proper generalization of the Mertens–Cesàro theorem to $\mathcal{O}$ (and not to the set of ideals of $\mathcal{O}$) the approach presented in [73] does not apply: indeed, given a large bound B, there might be infinitely many elements of norm at most B (contrary to what happens in the case of $\mathbb{Z}$). Therefore, not only

this definition of density for sets of ideals of $\mathcal{O}$ cannot extend to a definition of density for $\mathcal{O}$, but also the analogous probability interpretation that one has over $\mathbb{Z}$ is missing.

A *non canonical* definition for the density of a subset $A \subseteq \mathcal{O}$ is obtained by considering a $\mathbb{Z}$-isomorphism $\alpha\colon \mathcal{O} \to \mathbb{Z}^n$ (n being the degree of the extension $K \supseteq \mathbb{Q}$) and then by computing the density of $\alpha(A) \subseteq \mathbb{Z}^n$ as previously described. The resulting density is then dependent on the choice of α (which is equivalent to a choice of a $\mathbb{Z}$-basis for $\mathcal{O}$), but extends to $A \subseteq \mathcal{O}^m$ componentwise, as one would expect by considering the limit of the sequence $|\alpha(A) \cap [-B, B[^{mn}|/(2B)^{mn}$. Using this definition of density for the set $E \subseteq \mathcal{O}^m$ of coprime m-tuples and a similar strategy to the one presented in [48] for the case of unimodular matrices over $\mathbb{Z}$, the following turns out to be true:

- the density d of E exists and it can be computed;
- d is *independent* on the choice of the embedding α (i.e. independent of the choice of the $\mathbb{Z}$-basis for $\mathcal{O}$);
- d equals $1/\zeta_K(m)$, where $\zeta_K(m)$ is the Dedekind zeta function of the number field K.

This completely generalizes the Mertens–Cesàro theorem to the case of number fields. It is very interesting to note that this result matches the one presented in [73, Theorem 4.1], which was obtained in the context of ideals of $\mathcal{O}$.

Outline of the proof

Let us now briefly describe the strategy we use to compute the density mentioned above in the general case of a subset $E \subseteq \mathbb{Z}^M$ (in our case $M = nm$). First, we find a family $\{E_t\}_{t\in\mathbb{N}}$ of subsets of $\mathbb{Z}^M$ with the following properties:

- we are able to compute the density of E_t for every t (Lemma 4.3.5);
- $E_{t+1} \subseteq E_t$;
- $\bigcap_{t\in\mathbb{N}} E_t = E$.

Then we verify that the family of sets $\{E_t\}_{t\in\mathbb{N}}$ approximates the set E *in density* in the sense that the sequence of densities of $E_t \setminus E$ converges to zero as t tends to infinity. Under these assumptions we are able to prove that $\lim_{t\to\infty} \mathbb{D}(E_t) = \mathbb{D}(E)$ (Theorem 4.3.7).

4.1.1 Notation

If R is a ring (commutative with identity), we say that the ideals $I_1, \dots, I_l$ are coprime if $\sum_j I_j = R$; we say that the elements $a_1, \dots, a_s \in R$ are coprime if the ideals $(a_1), \dots, (a_s)$ are coprime. Let K be a number field of degree n and $\mathcal{O}$ its ring of algebraic integers. Let $\mathbb{E} = \{\mathbf{e}_i\}_{i=1}^n$ be a $\mathbb{Z}$-basis for $\mathcal{O}$. Define

$$\mathcal{O}[B, \mathbb{E}] = \left\{ \sum_{i=1}^{n} a_i \mathbf{e}_i \mid a_i \in [-B, B[\cap \mathbb{Z} \right\}.$$

Later on in the paper we will just write $\mathcal{O}[B]$ since the basis will be understood. For p a prime number, we denote by $S_p = \{\mathfrak{p}_1^{(p)}, \dots, \mathfrak{p}_{\lambda_p}^{(p)}\}$ the set of distinct prime ideals

lying over p (in particular we have that $\prod_{j=1}^{\lambda_p} \mathfrak{p}_j^{(p)}$ is the radical of the ideal generated by p). Let $d_j^{(p)}$ be the inertia degree of $\mathfrak{p}_j^{(p)}$ (i.e. $\dim_{\mathbb{F}_p}(\mathcal{O}/\mathfrak{p}_j^{(p)})$) and denote by D_p the integer $\sum_{j=1}^{\lambda_p} d_j^{(p)}$. Let d be a positive integer, let us denote by $\mathrm{GF}(p,d)$ the finite field of order p^d. Define

$$R_p \coloneqq \prod_{j=1}^{\lambda_p} \mathcal{O}/\mathfrak{p}_j^{(p)} \simeq \prod_{j=1}^{\lambda_p} \mathrm{GF}(p, d_j^{(p)}).$$

For $z = (z_1, \dots, z_m)$ an element of $\mathcal{O}^m$, we denote by I_z the ideal generated by the set $\{z_1, \dots, z_m\}$. If $\mathbb{F}$ is a field we denote by $\mathbb{F}^*$ its multiplicative group.

4.2 A definition of the density for $\mathcal{O}^m$

Let $\mathbb{E}$ be a $\mathbb{Z}$-basis for $\mathcal{O}$. Our goal is to define a notion of density (which will in general depend on the choice of $\mathbb{E}$) for a subset T of $\mathcal{O}^m$. We define the *upper density of T with respect to* $\mathbb{E}$ to be

$$\overline{\mathbb{D}_{\mathbb{E}}}(T) = \limsup_{B\to\infty} \frac{|\mathcal{O}[B,\mathbb{E}]^m \cap T|}{(2B)^{mn}}$$

and the *lower density of T with respect to* $\mathbb{E}$ as

$$\underline{\mathbb{D}_{\mathbb{E}}}(T) = \liminf_{B\to\infty} \frac{|\mathcal{O}[B,\mathbb{E}]^m \cap T|}{(2B)^{mn}}.$$

We say that T has *density d with respect to* $\mathbb{E}$ if

$$\overline{\mathbb{D}_{\mathbb{E}}}(T) = \underline{\mathbb{D}_{\mathbb{E}}}(T) =: \mathbb{D}_{\mathbb{E}}(T) = d.$$

Whenever this density is independent of the chosen basis $\mathbb{E}$, it is consistent to denote the density of a set T by $\mathbb{D}(T)$ without any subscript.

Remark 4.2.1. First observe that $d \in [0,1] \subseteq \mathbb{R}$ by construction. The main idea behind this definition of density is the same that one has over $\mathbb{Z}$; the only difference is that the way in which we cover the entire set (in this case $\mathcal{O}$) is not canonical but depends on the basis $\mathbb{E}$.

Example 4.2.2. Let us show with an example that choosing different bases for $\mathcal{O}$ could yield different densities for the same subset $T \subseteq \mathcal{O}$. Let $K = \mathbb{Q}(i)$, so that $\mathcal{O} = \mathbb{Z}[i]$. Let $T = \{x+iy \in \mathcal{O} \colon x, y > 0\}$. If $\mathbb{E} = \{1, i\}$, clearly $|\mathcal{O}[B,\mathbb{E}] \cap T| = (B-1)^2$, which gives $\mathbb{D}_{\mathbb{E}}(T) = 1/4$. On the other hand, choosing as a basis $\mathbb{E}' = \{1, -1+i\} = \{\mathbf{e}_1, \mathbf{e}_2\}$ we have that $T = \{x\mathbf{e}_1 + y\mathbf{e}_2 \in \mathcal{O} \colon x, y > 0,\ x > y\}$. Therefore $|\mathcal{O}[B,\mathbb{E}'] \cap T| = (B-1)(B-2)/2$, which shows that $\mathbb{D}_{\mathbb{E}'}(T) = 1/8$.

Let $E \subseteq \mathcal{O}^m$ be the set of coprime m-tuples, i.e. the elements $z \in \mathcal{O}^m$ for which $I_z = \mathcal{O}$. A corollary of our final result (Theorem 4.3.7) is that the density of E is actually independent of the basis $\mathbb{E}$: even though the choice of the covering of $\mathcal{O}^m$ is not canonical (it depends in fact on the chosen $\mathbb{Z}$-basis for $\mathcal{O}$) the density of E *is*.

4.3 Proof of the main result

Let $\mathbb{S}$ be a finite set of prime numbers. Let $E_{\mathbb{S}}$ be the set of m-tuples $z = (z_1, \dots, z_m)$ in $\mathcal{O}^m$ such that the ideal I_z is coprime with every $p \in \mathbb{S}$.

Remark 4.3.1. Equivalently, one checks that

$$E_{\mathbb{S}} = \{z \in \mathcal{O}^m \mid I_z + \mathfrak{p}_j^{(p)} = \mathcal{O} \quad \forall p \in \mathbb{S} \quad \text{and} \quad \forall j \in \{1, \dots, \lambda_p\}\}$$

by observing that $(p) \subseteq \prod_j \mathfrak{p}_j^{(p)}$ and the $\mathfrak{p}_j^{(p)}$ are maximal.

Let $\psi_p \colon (\mathcal{O}/(p))^m \to R_p^m = (\prod_{j=1}^{\lambda_p} \mathcal{O}/\mathfrak{p}_j^{(p)})^m$ be the morphism induced by the projection $\mathcal{O}/(p) \twoheadrightarrow \prod_{j=1}^{\lambda_p} \mathcal{O}/\mathfrak{p}_j^{(p)}$. Recall that $D_p = \sum_{j=1}^{\lambda_p} d_j^{(p)}$. In the following lemma and in Proposition 4.3.3 we will consider the surjection

$$\pi \colon \mathcal{O}^m \longrightarrow \left(\prod_{p \in \mathbb{S}} R_p\right)^m =: T$$

induced by the quotient maps $\mathcal{O} \to \mathcal{O}/\mathfrak{p}_j^{(p)}$. It is easy to prove the following lemma.

Lemma 4.3.2. We have

$$E_{\mathbb{S}} = \pi^{-1}\left(\prod_{p \in \mathbb{S}} \prod_{j=1}^{\lambda_p} \left(\left(\mathcal{O}/\mathfrak{p}_j^{(p)}\right)^m \setminus \{0\}\right)\right).$$

Proposition 4.3.3. Let q be a positive integer, $\mathbb{E}$ a $\mathbb{Z}$-basis for $\mathcal{O}$, $\mathbb{S}$ a finite set of prime numbers and $N = \prod_{p \in \mathbb{S}} p$. Then

$$|E_{\mathbb{S}} \cap \mathcal{O}[qN]^m| = (2q)^{mn} \prod_{p \in \mathbb{S}} \left(p^{nm - mD_p} \prod_{j=1}^{\lambda_p} (p^{d_j^{(p)} m} - 1)\right),$$

where $\mathcal{O}[qN]^m$ is the set of m-tuples of elements of $\mathcal{O}[qN]$.

Proof. The key point is to decompose the map π. For the rest of the proof, the reader may refer to the following diagram:

$$\begin{array}{ccccc} \mathcal{O}^m & \xrightarrow{\pi_N} & (\mathcal{O}/(N))^m & \xrightarrow{\overline{\psi}} & T \\ & & \| & & \| \\ & & (\prod_{p \in \mathbb{S}} \mathcal{O}/(p))^m & \xrightarrow{\psi} & (\prod_{p \in \mathbb{S}} R_p)^m \end{array}$$

where π_N is the quotient map, $\psi = (\dots, \psi_p, \dots)$ and $\overline{\psi}$ is its obvious extension to $(\mathcal{O}/(N))^m$ obtained by applying the Chinese remainder theorem to primes in $\mathbb{S}$. Notice then that $\pi = \overline{\psi} \circ \pi_N$. Our strategy to prove the result is to compute the cardinality of the fibers of ψ and the intersection of the fibers of π_N with $\mathcal{O}[qN]$:

- Observe that $\psi_p \colon (\mathcal{O}/(p))^m \to R_p^m$ is a surjective morphism of $\mathbb{F}_p$-vector spaces, therefore $|\psi_p^{-1}(y_p)| = |\ker(\psi_p)| = p^{nm - mD_p}$ for all $y_p \in R_p^m$. It follows that $|\overline{\psi}^{-1}(y)| = \prod_{p \in \mathbb{S}} |\psi_p^{-1}(y_p)| = \prod_{p \in \mathbb{S}} p^{nm - mD_p}$ for all $y \in (\mathcal{O}/(N))^m$.

- Let $\overline{z} = (\overline{z}_j)_j \in (\mathcal{O}/(N))^m$ and $z = (z_j)_j \in \mathcal{O}^m$. Write

$$\overline{z}_j = \left(\sum_{t=0}^{n} r_t^j \pi(\mathbf{e}_t) \right)$$

for some unique $0 \leq r_t^j < N$ in $\mathbb{Z}$. Observe that existence and uniqueness of the r_t^j follow from the fact that $\mathcal{O}/(N)$ is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank n with basis $\{\pi(\mathbf{e}_t)\}$. It follows that $\pi_N(z) = \overline{z}$ if and only if

$$z_j = \sum_{t=0}^{n} (r_t^j + l_t^j N)\mathbf{e}_t$$

for some $l_t^j \in \mathbb{Z}$. We conclude then that

$$|\mathcal{O}[qN]^m \cap \pi_N^{-1}(z)| = (2q)^{mn}$$

since the r_t^j are fixed by the condition $\pi_N(z) = \overline{z}$ and $l_t^j \in [-q, q[\cap\mathbb{Z}$ for each index j, t.

Let us now complete the proof. By Lemma 4.3.2 we have that

$$E_{\mathbb{S}} \cap \mathcal{O}[qN]^m = \pi^{-1} \left(\prod_{p \in \mathbb{S}} \prod_{j=1}^{\lambda_p} \left(\left(\mathcal{O}/\mathfrak{p}_j^{(p)} \right)^m \setminus \{0\} \right) \right) \cap \mathcal{O}[qN]^m. \tag{4.1}$$

In order to simplify the notation, define

$$H \coloneqq \psi^{-1} \left(\prod_{p \in \mathbb{S}} \prod_{j=1}^{\lambda_p} \left(\left(\mathcal{O}/\mathfrak{p}_j^{(p)} \right)^m \setminus \{0\} \right) \right),$$

so that $E_{\mathbb{S}} = \pi_N^{-1}(H)$ by Lemma 4.3.2. Since $\pi = \psi \circ \pi_N$, Equation (4.1) reads

$$E_{\mathbb{S}} \cap \mathcal{O}[qN]^m = \pi_N^{-1}(H) \cap \mathcal{O}[qN]^m.$$

Therefore

$$|\pi_N^{-1}(H) \cap \mathcal{O}[qN]^m| = (2q)^{mn}|H|$$

and

$$|H| = \prod_{p \in \mathbb{S}} \left(p^{nm - D_p m} \prod_{j=1}^{\lambda_p} \left| \left(\mathcal{O}/\mathfrak{p}_j^{(p)} \right)^m \setminus \{0\} \right| \right).$$

Thus,

$$|E_{\mathbb{S}} \cap \mathcal{O}[B]| = (2q)^{mn} \prod_{p \in \mathbb{S}} \left(p^{nm - mD_p} \prod_{j=1}^{\lambda_p} (p^{d_j^{(p)} m} - 1) \right).$$

□

Before we proceed, let us recall the following elementary calculus fact.

Lemma 4.3.4. Let $\{a_B\}_{B\in\mathbb{N}}$ be a sequence of real numbers and N a positive integer. Then

$$\lim_{B\to\infty} a_B = c \Leftrightarrow \lim_{q\to\infty} a_{r+qN} = c \quad \forall r \in \{0,\dots,N-1\}.$$

Lemma 4.3.5. In the notation previously described we have

$$\mathbb{D}(E_{\mathbb{S}}) = \mathbb{D}_{\mathbb{E}}(E_{\mathbb{S}}) = \prod_{p\in\mathbb{S}}\prod_{j=1}^{\lambda_p}\left(1-\frac{1}{p^{d_j^{(p)}m}}\right).$$

Proof. Let

$$a_B \coloneqq \frac{|\mathcal{O}[B]^m \cap E_{\mathbb{S}}|}{(2B)^{mn}}.$$

Recall that $N = \prod_{p\in\mathbb{S}} p$. Let

$$D \coloneqq \prod_{p\in\mathbb{S}}\prod_{j=1}^{\lambda_p}\left(1-\frac{1}{p^{d_j^{(p)}m}}\right).$$

We first show that $a_{qN} = D$. By Proposition 4.3.3 we have that

$$a_{qN} = \frac{|\mathcal{O}[qN]^m \cap E_{\mathbb{S}}|}{(2qN)^{mn}} =$$

$$= \frac{(2q)^{mn}\prod_{p\in\mathbb{S}} p^{nm-mD_p}\prod_{j=1}^{\lambda_p}(p^{d_j^{(p)}m}-1)}{(2qN)^{mn}}.$$

By canceling common factors in numerator and denominator and writing D_p according to its definition we get

$$a_{qN} = \prod_{p\in\mathbb{S}} p^{-m\sum_{j=1}^{\lambda_p} d_j^{(p)}} \prod_{j=1}^{\lambda_p}(p^{d_j^{(p)}m}-1)$$

and bringing $p^{-m\sum_{j=1}^{\lambda_p} d_j^{(p)}}$ inside the products it follows that

$$a_{qN} = \prod_{p\in\mathbb{S}}\prod_{j=1}^{\lambda_p}\left(1-\frac{1}{p^{d_j^{(p)}m}}\right).$$

We are now ready to prove that

$$\lim_{B\to\infty} a_B = D.$$

Thanks to Lemma 4.3.4 it will be enough to show that

$$\lim_{q\to\infty} a_{r+qN} = D$$

for all $r \in \{0,\dots,N-1\}$. Indeed,

$$a_{qN}\cdot\left(\frac{(2qN)}{2r+2qN}\right)^{mn} < a_{r+qN} < a_{(q+1)N}\cdot\left(\frac{(2(q+1)N)}{2r+2qN}\right)^{mn}.$$

By passing to the limit in q the claim follows. □

Remark 4.3.6. It is immediate to observe that the density of $E_{\mathbb{S}}$ is independent of the chosen basis $\mathbb{E}$.

We are now in a position to formulate and prove the main result.

Theorem 4.3.7. Let m be a positive integer and let K be a number field. Let $\mathcal{O}$ be the ring of integers of K. The density of the set E of coprime m-tuples of $\mathcal{O}$ is

$$\mathbb{D}(E) = \frac{1}{\zeta_K(m)},$$

where ζ_K is the Dedekind zeta function of the number field K.

Remark 4.3.8. Let $p_1, \dots, p_t$ be the first t rational primes. We define $\mathbb{S}_t = \{p_1, \dots, p_t\}$. The reader should observe that one has the inclusion $E \subseteq E_{\mathbb{S}_t}$ and therefore

$$0 \leq \mathbb{D}_{\mathbb{E}}(E) \leq \overline{\mathbb{D}_{\mathbb{E}}}(E) \leq \mathbb{D}(E_{\mathbb{S}_t}).$$

As a consequence one has that in the case $m = 1$ Theorem 4.3.7 follows by passing to the limit $t \to \infty$ in the above inequality and recalling that the Dedekind zeta function of K has a pole at 1. As expected in fact, the group of units of the ring of integers has density zero in any basis. Observe that this is the special case $k = 1$ of [12, Corollary 4.2]. A more extensive description of additive representations of elements in the unit group can be found in [3].

Remark 4.3.9. Notice that the argument of 4.3.8 does not lead to the conclusion in the case $m > 1$, since it provides just an upper bound (uniform in $\mathbb{E}$) for $\overline{\mathbb{D}_{\mathbb{E}}}(E)$.

Before starting the proof let us recall the following theorem, which we will use as a fundamental tool.

Theorem 4.3.10 ([47, Lemma 2])**.** Let $S \subseteq \mathbb{R}^M$ be a bounded set whose boundary ∂S can be covered by the images of at most W maps $\phi\colon [0,1]^{M-1} \to \mathbb{R}^M$ satisfying Lipschitz conditions

$$|\phi(x) - \phi(y)| \leq L|x - y|$$

for the Euclidean norm. Then S is measurable. Let $V = \mathrm{vol}(S)$.

Let $\Lambda \subseteq \mathbb{R}^M$ be a full-rank lattice and

$$\lambda_1 \coloneqq \inf\{|v|\colon v \in \Lambda \setminus \{0\}\}$$

be its first successive minimum. Then

$$\left| |\Lambda \cap S| - \frac{V}{\det \Lambda} \right| \leq cW \left(\frac{L}{\lambda_1} + 1 \right)^{M-1}$$

for a constant c depending only on M.

Next we are going to deduce from Theorem 4.3.10 the particular case that we will use in the proof of Theorem 4.3.7.

Proposition 4.3.11. Let K be a number field of degree n with ring of integers $\mathcal{O}$. Let I be an ideal of $\mathcal{O}$. Then

$$\left| |(I \cap \mathcal{O}[B])^m| - \frac{(2B)^{nm}}{N(I)^m} \right| \leq c \left(\frac{2B}{c_1 N(I)^{1/n}} + 1 \right)^{mn-1}$$

for every $B \in \mathbb{N}$, where $N(I)$ denotes the norm of I and the constants c, c_1 are independent of B and of I.

Proof. Recall that there is a canonical embedding of $\mathcal{O}$ into $\mathbb{R}^n$: if $\sigma_1, \dots, \sigma_r$ are the real embeddings $K \to \mathbb{R}$ and $\sigma_{r+1}, \dots, \sigma_{r+2s} = \sigma_n$ are the complex ones labeled such that $\sigma_{r+i} = \overline{\sigma_{r+s+i}}$, then the map $\tau \colon \mathcal{O} \to \mathbb{R}^n$ defined by

$$x \mapsto (\sigma_1(x), \dots, \sigma_r(x), \sigma_{r+1}(x), \dots, \sigma_{r+s}(x))$$

embeds $\mathcal{O}$ as a full-rank lattice in $\mathbb{R}^n$, where each σ_{r+i} is viewed as an embedding into $\mathbb{R}^2$. The map τ induces an embedding $\tau^m \colon \mathcal{O}^m \to \mathbb{R}^{mn}$. The image of $\mathcal{O}^m$ inside $\mathbb{R}^{mn}$ via τ^m is again a full-rank lattice. Let $\alpha_{\mathbb{E}} \colon \mathcal{O} \longrightarrow \mathbb{Z}^n$ be the isomorphism of $\mathbb{Z}$-modules given by $\alpha_{\mathbb{E}} \left(\sum_{i=1}^n x_i \mathbf{e}_i \right) = (x_1, \dots, x_n)$. Let $\alpha_{\mathbb{E}}^m \colon \mathcal{O}^m \to \mathbb{Z}^{mn}$ be the isomorphism induced by $\alpha_{\mathbb{E}}$. Consider the following commutative diagram

$$\begin{array}{ccc} \mathcal{O}^m & \xrightarrow{\tau^m} & \mathbb{R}^{mn} \\ {\scriptstyle \alpha_{\mathbb{E}}^m}\downarrow & & \uparrow{\scriptstyle A} \\ \mathbb{Z}^{mn} & \xrightarrow{\iota} & \mathbb{R}^{mn} \end{array}$$

where ι is the inclusion map and A is the unique $\mathbb{R}$-linear map which makes the diagram commute. The idea now is to apply Theorem 4.3.10 with $\Lambda = (\iota \circ \alpha_{\mathbb{E}}^m)(I^m) \subseteq \mathbb{R}^{mn}$ and S the cube of side $2B$ centered in the origin, so that $W = 2mn$ and $L = 2B$ in the notation of the theorem. Here by I^m we mean the cartesian product of m copies of I inside $\mathcal{O}^m$.

We first need a lower bound for the first successive minimum of $(\iota \circ \alpha_{\mathbb{E}}^m)(I^m)$. To do this we can clearly assume $m = 1$ since the first successive minimum of a lattice $\Lambda \subseteq \mathbb{R}^n$ coincides with that of $\Lambda^m \subseteq \mathbb{R}^{mn}$. Let v be a vector realizing the first successive minimum of $(\iota \circ \alpha_{\mathbb{E}})(I)$ with respect to the euclidean norm $|\cdot|$. By [47, Lemma 5], the first successive minimum of $\tau(I)$ is greater or equal than $N(I)^{1/n}$. Since $A(v) \in \tau(I)$ we have that

$$N(I)^{1/n} \leq |A(v)| \leq \|A\| |v|,$$

where $\|A\|$ is defined by $\sup_{|w|=1} |A(w)|$. This shows that the first successive minimum of $(\iota \circ \alpha_{\mathbb{E}})(I)$ is greater or equal than $c_1 N(I)^{1/n}$, where $c_1 \coloneqq 1/\|A\|$ is independent of B and of I.

Now the claim follows by applying Theorem 4.3.10 together with the fact that

$$\det(\alpha_{\mathbb{E}}^m(I^m)) = \det(\alpha_{\mathbb{E}}(I))^m = [\mathbb{Z}^n \colon \alpha_{\mathbb{E}}(I)]^m = [\mathcal{O} \colon I]^m = N(I)^m$$

and observing that $|(\iota \circ \alpha_{\mathbb{E}}^m)(I^m) \cap [-B, B[^{mn}| = |I^m \cap \mathcal{O}[B]^m| = |(I \cap \mathcal{O}[B])^m|$. □

Proof of Theorem 4.3.7. We already proved the theorem in the case $m = 1$ in Remark 4.3.8, therefore let us suppose $m > 1$. Let t be a positive integer, $\mathbb{S}_t$ the set consisting of the first t prime numbers and define $E_t = E_{\mathbb{S}_t}$. Observe that, since $E_t \supseteq E$, we have

$$\overline{\mathbb{D}_{\mathbb{E}}}(E) \leq \overline{\mathbb{D}}(E_t) = \mathbb{D}(E_t).$$

By letting t run to infinity we get

$$\overline{\mathbb{D}_{\mathbb{E}}}(E) \leq \frac{1}{\zeta_K(m)}.$$

In order to show the opposite inequality observe that

$$\mathbb{D}(E_t) - \overline{\mathbb{D}_{\mathbb{E}}}(E_t \setminus E) \leq \underline{\mathbb{D}_{\mathbb{E}}}(E). \tag{4.2}$$

Therefore, it is enough to prove that $\lim_{t\to\infty} \overline{\mathbb{D}_{\mathbb{E}}}(E_t \setminus E) = 0$. For a prime ideal $\mathfrak{p} \subseteq \mathcal{O}$, the t-th prime number p_t and M an integer, let us introduce the following notation.

- We say that $\mathfrak{p} \succ M$ if and only if $\mathfrak{p}$ lies over a prime greater than M (Notice that, with this notation, one has that $\mathfrak{p} \succ p_t$ implies $\mathfrak{p} + (p_i) = \mathcal{O}$ for every $i \leq t$).
- We say that $M \succ \mathfrak{p}$ if and only if the rational prime lying under $\mathfrak{p}$ is less than M.

If $\mathcal{P}$ is the set of prime ideals of $\mathcal{O}$, with this notation we have

$$E_t \setminus E \subseteq \bigcup_{\mathfrak{p}\in\mathcal{P}\colon \mathfrak{p}\succ p_t} \mathfrak{p}^m \subseteq \mathcal{O}^m,$$

where $\mathfrak{p}^m$ is the set m-tuples of elements of $\mathcal{O}$ having all entries in $\mathfrak{p}$. It follows that

$$(E_t \setminus E) \cap \mathcal{O}[B]^m \subseteq \bigcup_{\mathfrak{p}\in\mathcal{P}\colon CB^n\succ\mathfrak{p}\succ p_t} (\mathfrak{p} \cap \mathcal{O}[B])^m$$

for C a positive constant independent of B. The upper bound $CB^n \succ \mathfrak{p}$ comes from the following observation: for a fixed basis $\mathbb{E}$, the norm function is a polynomial of degree n in the coefficients (with respect to the basis $\mathbb{E}$) of the elements of $\mathcal{O}$. Therefore $N(\mathcal{O}[B]) \subseteq [-CB^n, CB^n]$ for a constant C depending only on the chosen basis. On the other hand, if an element of $\mathcal{O}[B]$ is in $\mathfrak{p}$ then its norm is divisible by the rational prime p lying under $\mathfrak{p}$. This shows that there cannot exist primes $\mathfrak{p} \succ CB^n$ containing a non-zero element of $\mathcal{O}[B]$. We have then

$$\begin{aligned}\overline{\mathbb{D}_{\mathbb{E}}}(E_t \setminus E) &\leq \limsup_{B\to\infty} \left| \bigcup_{\mathfrak{p}\in\mathcal{P}\colon CB^n\succ\mathfrak{p}\succ p_t} \mathfrak{p}^m \cap \mathcal{O}[B]^m \right| \cdot (2B)^{-nm} \\ &\leq \limsup_{B\to\infty} \sum_{\mathfrak{p}\in\mathcal{P}\colon CB^n\succ\mathfrak{p}\succ p_t} |\mathfrak{p} \cap \mathcal{O}[B]|^m \cdot (2B)^{-nm}.\end{aligned}$$

By Proposition 4.3.11, $|\mathfrak{p}\cap\mathcal{O}[B]|^m = |(\mathfrak{p}\cap\mathcal{O}[B])^m| \leq \frac{(2B)^{mn}}{N(\mathfrak{p})^m} + c\left(\frac{2B}{c_1 N(\mathfrak{p})^{1/n}} + 1\right)^{mn-1}$. Therefore

$$\begin{aligned}\overline{\mathbb{D}}_{\mathbb{E}}(E_t \setminus E) &\leq \limsup_{B\to\infty} \sum_{CB^n\succ\mathfrak{p}\succ p_t} |\mathfrak{p} \cap \mathcal{O}[B]|^m \cdot (2B)^{-nm} \\ &\leq \limsup_{B\to\infty} \sum_{CB^n\succ\mathfrak{p}\succ p_t} \frac{1}{N(\mathfrak{p})^m} + c\left(\frac{2B}{c_1 N(\mathfrak{p})^{1/n}} + 1\right)^{mn-1} \cdot (2B)^{-nm} \\ &\leq \limsup_{B\to\infty} \sum_{CB^n>p>p_t} \frac{n}{p^m} + cn\left(\frac{2B}{c_1 p^{1/n}} + 1\right)^{mn-1} \cdot (2B)^{-nm} \\ &=: L_t,\end{aligned}$$

where the last inequality holds because in each instance $N(\mathfrak{p}) \geq p$ for p the prime below $\mathfrak{p}$, and above a fixed rational prime lie at most n distinct primes of $\mathcal{O}$. Now our goal is to show that $L_t \to 0$ as $t \to \infty$.

Choose now a constant $c_1' \leq c_1$ (independent of B) for which $\frac{1}{C^{1/n}} \geq \frac{c_1'}{2}$. Notice that the sum that appears in L_t is taken over primes p such that $CB^n > p$, which shows that

$$B > \frac{1}{C^{1/n}} p^{1/n} \geq \frac{c_1'}{2} p^{1/n}.$$

It follows $\frac{2B}{c_1' p^{1/n}} \geq 1$ and then $\frac{2B}{c_1' p^{1/n}} + 1 \leq 2\frac{2B}{c_1' p^{1/n}}$. Therefore L_t is bounded by

$$\limsup_{B\to\infty} \sum_{p:\, CB^n > p > p_t} \frac{n}{p^m} + cn \left(\frac{4B}{c_1' p^{1/n}}\right)^{mn-1} \cdot (2B)^{-nm} =$$

$$= \limsup_{B\to\infty} \sum_{p:\, CB^n > p > p_t} \frac{n}{p^m} + \frac{c'}{B \cdot p^{m-1/n}}$$

for some other constant c' independent of B and p. Now observe that

$$\limsup_{B\to\infty} \sum_{p:\, CB^n > p > p_t} \frac{n}{p^m} \leq \sum_{p > p_t} \frac{n}{p^m}$$

tends to zero when $t \to \infty$ because the series $\sum_p \frac{1}{p^m}$ is convergent, while for the other term one has that

$$\limsup_{B\to\infty} \sum_{CB^n > p > p_t} \frac{c'}{B \cdot p^{m-1/n}} \leq \limsup_{B\to\infty} \frac{c'}{B} \sum_{CB^n > p > p_t} \frac{1}{p} = 0$$

since $\sum_{p < CB^n} \frac{1}{p}$ is asymptotic to $\log\log(CB^n)$. This concludes the proof by equation (4.2).

□

The following corollary produces the classical generalization of Mertens–Cesàro theorem to the case of m-tuples of integers (presented in [57]).

Corollary 4.3.12 (Extended Mertens–Cesàro theorem)**.** The density of coprime m-tuples of integers is $\frac{1}{\zeta(m)}$, where ζ is the Riemann zeta function.

Proof. Follows directly from Theorem 4.3.7 by setting $K = \mathbb{Q}$. □

Remark 4.3.13. Observe that the results of Theorem 4.3.7 are consistent with the expectations. The obtained density is in fact independent of the basis: by symmetry, indeed, all proofs can be done by using another basis $\mathbb{B}$, obtaining the same result. In addition, Theorem 4.3.7 extends the Mertens–Cesàro theorem for algebraic integers in the following sense: over $\mathbb{Z}$ one can equivalently consider the density of the set of coprime m-tuples of integers or coprime m-tuples of ideals of $\mathbb{Z}$ without any relevant distinction. If one is willing to do the same in the case of algebraic integers, one has to choose in which context one wants to consider the problem: in the context of m-tuples of ideals,

the results in [73] are satisfying while in the setting of m-tuples of algebraic integers, Theorem 4.3.7 answers the question. Curiously, even if the set up of the problem is very different, the resulting densities match. Future work in this direction could possibly include an analysis of the density of r-prime m-tuples of algebraic integers, extending the definition given by Sittinger in [73].

Remark 4.3.14. In [64] the author gives an asymptotic for the number of points of bounded height B in the $(m-1)$-dimensional projective space. We will briefly explain why this result goes in a similar direction as the ones in the present note. Let E be the set of coprime m-tuples of $\mathcal{O}_K^m$. There is an action of the group of units $\mathcal{O}_K^*$ on E given by $u(c_1, ..., c_m) = (uc_1, ..., uc_m)$ if $u \in \mathcal{O}_K^*$ and $(c_1, ..., c_m) \in E$. The natural map from E to the $(m-1)$-dimensional projective space $\mathbb{P}_K^{m-1}$ induces an injection ι from $E/\mathcal{O}_K^*$ to $\mathbb{P}_K^{m-1}$. When K has class number one, ι is also a surjection; now one could use [64, Theorem 3] to see that the number of elements of $E/\mathcal{O}_K^*$ of bounded height B is asymptotic to $C_m(K)B^m/\zeta_K(m)$ where $C_m(K)$ is a constant depending on m and the number field K. Schanuel gets the constants because he is essentially "counting" more objects. For example, when $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ the point $Q = [1 + \sqrt{-5}, 2] \in \mathbb{P}_K^1$ would be "counted" in the case of Schanuel's result even though Q is not proportional to a coprime m-tuple. This happens because the class number of K is different from 1.

Acknowledgements

The authors would like to thank Fabrizio Barroero for his suggestion of using Theorem 4.3.10. We also want to thank Francesco Monopoli and Reto Schnyder for useful comments. Moreover, we are grateful to the anonymous referee for the suggestions, which helped us to improve the structure and the content of the paper.

Appendix A

Computing the newform attached to a quadratic $\mathbb{Q}$-curve

In what follows, we show how we implemented the algorithm described in section 2.4 which computes, given a quadratic $\mathbb{Q}$-curve E completely defined over a quadratic field K, a newform $f = \sum_{n\geq 1} a_n q^n$ in $S_2(\Gamma_1(N), \varepsilon)$, for suitable N, ε, such that $L(E/K, s) = L(f, s)L({}^{\sigma}f, s)$. The code below was implemented in Sage [75].

We divided the code into blocks of functions which all contribute to the same task. Below every block, we describe the input and the output of the main function of the block, which is always the first one.

The following variables are the same for the main function of each block. Therefore we omit them from the description of the input.

- `E` - the $\mathbb{Q}$-curve we start with;
- `K` - the base field of E;
- `Ec` - the Galois conjugate ${}^{\nu}E$ of E;
- `mu` - an isogeny $\mu\colon E \to {}^{\nu}E$;
- `m` - the integer which coincides with ${}^{\nu}\mu \circ \mu$;
- `M` - the number field $\mathbb{Q}(\sqrt{m})$.

```
def E_newform(E,mu,prec):
    m = mu.formal()[1].norm()
    K= E.base()
    R.<x> = QQ[]
    M.<b>=NumberField(x^2-m)
    a=K.gen()
    nu=K.automorphisms()[1]
    Ec=E.base_extend(nu)
    d=K.disc().abs()
    N=ZZ(E.conductor().norm().sqrt())*d
```

```
    t=[0,1]
    for i in IntegerRange(2,prec+1):
        if i.is_prime():
            t.append(ap(E,Ec,K,nu,i,mu,M,epsilon(N,K,i,m)))
        else:
            t.append(1)
            u=i.factor()
            for j in u:
                if j[1]==1:
                    t[i]=t[i]*t[j[0]]
                else:
                    t[i]=t[i]*(t[j[0]]*t[j[0]^(j[1]-1)]
                         -epsilon(N,K,j[0],m)*j[0]
                         *t[j[0]^(j[1]-2)])
    return t

def epsilon(N,K,p,m):
    if p.divides(N):
        return 0
    elif m>0 or len(K.primes_above(p))==2:
        return 1
    elif len(K.primes_above(p))==1:
        return -1

def ap(E,Ec,K,nu,p,mu,M,epsilon):
    P=K.primes_above(p)[0]
    if E.has_bad_reduction(P):
        if E.has_additive_reduction(P):
            return 0
        elif len(P)==1:
            return bad_inert(E,Ec,nu,mu,p,P)*M.gen()
        elif len(P)==2:
            if E.has_split_multiplicative_reduction(P):
                return 1
            elif E.has_nonsplit_multiplicative_reduction(P):
                return -1
    else
        if p.divides(K.discriminant()):
            return ramified(E,Ec,nu,mu,M,p,P)
        elif len(P)==1:
            return inert(E,Ec,nu,mu,M,p,P,epsilon)
        elif len(P)==2:
            Ep = E.local_minimal_model(P).reduction(P)
            return Ep.trace_of_frobenius()
```

INPUT:

- `prec` - a positive integer.

OUTPUT:

- a list $[a_0, \ldots, a_{\text{prec}}]$ of Fourier coefficients of f.

```
def reduce_isogeny(K,mu,P,F):
    MU=mu.rational_maps()
    f=MU[0].numerator()
    g=MU[0].denominator()
    f1=MU[1].numerator()
    g1=MU[1].denominator()
    r=f.coefficients()
    s=f1.coefficients()
    v=r[0].valuation(P)
    min=r[0]
    for i in r:
        z=i.valuation(P)
        if z<v:
            v=z
            min=i
    f_red=f/min
    g_red=g/min
    v=s[0].valuation(P)
    min=s[0]
    for i in s:
        z=i.valuation(P)
        if z<v:
            v=z
            min=i
    f1_red=f1/min
    g1_red=g1/min
    return [F(f_red.dict())/F(g_red.dict()),
            F(f1_red.dict())/F(g1_red.dict())]
```

INPUT:

- `P` - a prime ideal of the ring of integers $\mathcal{O}_K$ of K;
- `F` - the field $(\mathcal{O}_K/\texttt{P})(x, y)$.

OUTPUT:

- a pair of rational functions in $(\mathcal{O}_K/\texttt{P})(x, y)$ which give the reduction of μ modulo `P`.

```
def apply_isogeny(Ep,mup,Q):
    try:
        return Ep(mup[0](Q[0],Q[1]),mup[1](Q[0],Q[1]))
    except ZeroDivisionError:
        return Ep(0)
```

INPUT:

- `Ep` - an elliptic curve over a finite field;
- `mup` - an isogeny of `Ep`;
- `Q` - a rational point of `Ep`.

OUTPUT:

- the image of `Q` via `mup`.

```
def bad_inert(E,Ec,nu,mu,p,P):
    phi=copy(mu)
    R=P.residue_field()
    F=FractionField(R['x','y'])
    Em=E.local_minimal_model(P)
    Emc=Em.base_extend(nu)
    iso1=Em.isomorphisms(E)[0]
    iso2=Ec.isomorphisms(Emc)[0]
    phi.set_post_isomorphism(iso2)
    phi.set_pre_isomorphism(iso1)
    Emp=[R(Em.a1()),R(Em.a2()),R(Em.a3()),
         R(Em.a4()),R(Em.a6())]
    Empc=[R(Emc.a1()),R(Emc.a2()),R(Emc.a3()),
          R(Emc.a4()),R(Emc.a6())]
    phi_red=reduce_isogeny(K,phi,P,F)
    while True:
        Q=randompt(Emp,R)
        Qp=(Q[0]^p,Q[1]^p)
        phi_Q=(phi_red[0](Q[0],Q[1]),phi_red[1](Q[0],Q[1]))
        phi_Q = mul_p(p,phi_Q, Empc)
        phi_Q_inv=(phi_Q[0],-phi_Q[1]-Empc[0]*phi_Q[0]
                   -Empc[2])
        if Qp!=phi_Q or Qp!=phi_Q_inv:
            break
    if Qp==phi_Q:
        return 1
    elif Qp==phi_Q_inv:
        return -1
    else:
        raise RuntimeError

def randompt(R,Emp):
    S.<z>=R[]
    l=[]
    c=0
        while len(l)==0 or c==0:
```

```
            k=R.random_element()
            f=z^2+Emp[0]*k*z+Emp[2]*z-k^3-Emp[1]*k^2
              -Emp[3]*k-Emp[4]
            l=f.roots()
            if len(l)!=0:
                c=2*l[0][0]+Emp[0]*k+Emp[2]
    return (k,l[0][0])

def mul_p(p,P,E):
    p2=p.binary()
    l=len(p2)
    Q=P
    S=P
    for i in IntegerRange(0,l-1):
        Q=add(Q,Q,E)
        if p2[l-2-i]=='1':
            S=add(Q,S,E)
    return S

def add(P,Q,E):
    if P[0]!=Q[0]:
        l=(Q[1]-P[1])/(Q[0]-P[0])
        nu=(P[1]*Q[0]-Q[1]*P[0])/(Q[0]-P[0])
    else:
        l=(3*P[0]^2+2*E[1]*P[0]+E[3]-E[0]*P[1])
           /(2*P[1]+E[0]*P[0]+E[2])
        nu=(-P[0]^3+E[3]*P[0]+2*E[4]-E[2]*P[1])
            /(2*P[1]+E[0]*P[0]+E[2])
    x3=l^2+E[0]*l-E[1]-P[0]-Q[0]
    y3=-(l+E[0])*x3-nu-E[2]
    return (x3,y3)
```

INPUT:

- `p` - a rational prime, inert in K, such that E has non-split multiplicative reduction at `p`;
- `P` - the unique prime of $\mathcal{O}_K$ lying above `p`.

OUTPUT:

- the sign of $a_p/\sqrt{m}$ (see section 2.4).

```
def inert(E,Ec,nu,mu,M,p,P,epsilon):
    phi=copy(mu)
    R=P.residue_field()
    F=FractionField(R['x','y'])
    Em=E.local_minimal_model(P)
```

```
    Ep=Em.reduction(P)
    aP=Ep.trace_of_frobenius()
    ap=M(aP+2*epsilon*p)
    if ap==0:
        return 0
    else:
        Emc=Em.base_extend(nu)
        Epc=Emc.reduction(P)
        iso1=Em.isomorphisms(E)[0]
        iso2=Ec.isomorphisms(Emc)[0]
        phi.set_post_isomorphism(iso2)
        phi.set_pre_isomorphism(iso1)
        phi_red=reduce_isogeny(K,phi,P,F)
        c=ZZ(ap.sqrt()/M.gen())
        q1=0
        q2=0
        while True:
            Q=Epc.random_point()
            if Q==0:
                continue
            q2=isog_inert(Epc,phi_red,p,Q,-c,epsilon)
            q1=isog_inert(Epc,phi_red,p,Q,c,epsilon)
            if q1==1 or q2==1:
                break
        if q1==0:
            return c*M.gen()
        else:
            return -c*M.gen()

def isog_inert(Epc,mu_red,p,Q,c,epsilon):
    Qp=Q-c*apply_isogeny(Epc,mu_red,(Q[0]^p,Q[1]^p))
       +epsilon*p*Q
    if Qp==0:
        return 0
    else:
        return 1
```

INPUT:

- `nu` - the non-trivial automorphism of K;
- `p` - a rational prime, inert in K, of good reduction for E;
- `P` - the unique prime lying above `p`;
- `epsilon` - the value $\varepsilon(p)$.

OUTPUT:

- the Fourier coefficient a_p.

```
def ramified(E,Ec,nu,mu,M,p,P):
    phi=copy(mu)
    R=P.residue_field()
    F=FractionField(R['x','y'])
    Em=E.local_minimal_model(P)
    Ep=Em.reduction(P)
    Emc=Em.base_extend(nu)
    Epc=Emc.reduction(P)
    iso1=Em.isomorphisms(E)[0]
    iso2=Ec.isomorphisms(Emc)[0]
    phi.set_post_isomorphism(iso2)
    phi.set_pre_isomorphism(iso1)
    phi_red=reduce_isogeny(K,phi,P,F)
    aP=Ep.trace_of_frobenius()
    t=M(aP^2-4*p)
    c=ZZ(t.sqrt()/M.gen())
    q1=0
    q2=0
    while True:
        Q=Ep.random_point()
        if Q==0:
            continue
        q1=isog_ramified(Ep,phi_red,p,Q,aP,c)
        if q1==1:
            break
        q2=isog_ramified(Ep,phi_red,p,Q,aP,-c)
        if q2==1:
            break
    if q1==0:
        return (aP+c*M.gen())/2
    else:
        return (aP-c*M.gen())/2

def isog_ramified(Ep,mu_red,p,Q,aP,c):
    Qp=2*Q-aP*Q-c*apply_isogeny(Ep,mu_red,Q)
    if Qp==0:
        return 0
    else:
        return 1
```

INPUT:

- `nu` - the non-trivial automorphism of K;
- `p` - a rational prime, ramified in K, of good reduction for E;
- `P` - the unique prime lying above `p`;

OUTPUT:

- the Fourier coefficient a_p.

Bibliography

[1] A. Abbes and E. Ullmo. À propos de la conjecture de Manin pour les courbes elliptiques modulaires. *Compositio Math.*, 103(3):269–286, 1996.

[2] A. O. L. Atkin and W. Li. Twists of newforms and pseudo-eigenvalues of W-operators. *Invent. Math.*, 48(3):221–243, 1978.

[3] F. Barroero, C. Frei, and R. Tichy. Additive unit representations in rings over global fields - a survey. *Publ. Math. Debrecen*, 79(3):291–307, 2011.

[4] B. Bektemirov, B. Mazur, W. Stein, and M. Watkins. Average ranks of elliptic curves: tension between data and conjecture. *Bull. Amer. Math. Soc. (N.S.)*, 44(2):233–254, 2007.

[5] N. Billerey. Critères d'irréductibilité pour les représentations des courbes elliptiques. *Int. J. Number Theory*, 7(4):1001–1032, 2011.

[6] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*. Springer-Verlag, 1990.

[7] J. G. Bosman, P. J. Bruin, A. Dujella, and F. Najman. Ranks of elliptic curves with prescribed torsion over number fields. *Int. Math. Res. Not. IMRN*, 11:2885–2923, 2014.

[8] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[9] A. F. Brown and E. P. Ghate. Endomorphism algebras of motives attached to elliptic modular forms. *Ann. de l'Inst. Fourier*, 53(6):1615–1676, 2003.

[10] H. Carayol. Sur les représentations l-adiques associées aux formes modulaires de Hilbert. *Ann. sci. E.N.S*, 19(3):409–468, 1986.

[11] H. Carayol. Sur les représentations galoisiennes modulo l attachées aux formes modulaires. *Duke Math. J.*, 59(3):785–801, 1989.

[12] F. Cellarosi and I. Vinogradov. Ergodic properties of k-free integers in number fields. *J. Modern Dynamics*, 7(3):461–488, 2013.

[13] E. Cesàro. Question proposée 75. *Mathesis 1*, 184, 1881.

[14] E. Cesàro. Question 75 (solution). *Mathesis*, 3, 1883.

[15] H. Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics. Springer, 1993.

[16] J. Cremona and T. Thongjunthug. The complex AGM, periods of elliptic curves over $\mathbb{C}$ and complex elliptic logarithms. *J. Number Theory*, 133(8):2813–2841, 2010.

[17] H. Darmon, V. Rotger, and Y. Zhao. The Birch and Swinnerton-Dyer conjecture for $\mathbb{Q}$-curves and Oda's period relations. In *Geometry and analysis of automorphic forms of several variables*, volume 7 of *Ser. Number Theory Appl.*, pages 1–40. World Sci. Publ., Hackensack, NJ, 2012.

[18] P. Deligne. Formes modulaires et représentations l-adiques. In *Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363*, volume 175 of *Lecture Notes in Math.*, pages Exp. No. 355, 139–172. Springer, Berlin, 1971.

[19] P. Deligne and J.-P. Serre. Formes modulaires de poids 1. *Ann. Scient. de l'E.N.S.*, 7(4):507–530, 1974.

[20] F. Diamond and J. Shurman. *A First Course in Modular Forms*, volume 228 of *GTM*. Springer, 2005.

[21] T. Dokchitser. Computing special values of motivic L-functions. *Exper. Math.*, 13(2):137–149, 2004.

[22] T. Dokchitser. computeL. `http://www.maths.bris.ac.uk/~matyd/computel/index.html`, 2006.

[23] T. Dokchitser. Notes on the parity conjecture. In *Elliptic curves, Hilbert modular forms and Galois deformations*, Adv. Courses Math. CRM Barcelona, pages 201–249. Birkhäuser/Springer, Basel, 2013.

[24] V.G. Drinfel'd. Two theorems on modular curves. *Funkts. Anal. Prilozh.*, 7:83–84, 1973.

[25] B. Edixhoven. On the Manin constants of modular elliptic curves. *Progr. Math.*, 89:25–39, 1989.

[26] B. Edixhoven. Néron models and tame ramification. *Compositio Math.*, 81(3):291–306, 1992.

[27] N. D. Elkies. On elliptic K-curves. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 81–91. Birkhäuser, Basel, 2004.

[28] J. Ellenberg. $\mathbb{Q}$-curves and Galois representations. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 93–103. Birkhäuser, Basel, 2004.

[29] D. Goldfeld. On the computational complexity of modular symbols. *Math. of Comp.*, 58(198):807–814, 1992.

[30] J. González and J.-C. Lario. $\mathbb{Q}$-curves and their Manin ideals. *Amer. J. Math.*, 123(3):475–503, 2001.

[31] E. González-Jiménez and X. Guitart. On the modularity level of modular abelian varieties over number fields. *J. Number Theory*, 130:1560–1570, 2010.

[32] B. H. Gross. Kolyvagin's work on modular elliptic curves. *London Math. Soc. Lecture Note Ser.*, 153:235–256, 1991.

[33] B. H. Gross. Lectures on the conjecture of Birch and Swinnerton-Dyer. In *Arithmetic of L-functions*, volume 18 of *IAS/Park City Math. Ser.*, pages 169–209. Amer. Math. Soc., Providence, RI, 2011.

[34] B. H. Gross and D. B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[35] X. Guitart and J. Quer. Modular abelian varieties over number fields. *Canad. J. Math.*, 66(1):170–196, 2014.

[36] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Clarendon Press Oxford, 1960.

[37] Y. Hasegawa. $\mathbb{Q}$-curves over quadratic fields. *Manuscripta Math.*, 94:347–364, 1997.

[38] U. Jannsen. The splitting of the Hochschild-Serre spectral sequence for a product of groups. *Canad. Math. Bull.*, 33:181–183, 1990.

[39] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

[40] I. Kiming. Explicit classification of some 2-extensions of a field of characteristic different from 2. *Canad. J. Math.*, XLII(5):825–855, 1990.

[41] V. Kolyvagin. Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves. *(transl.) Math. USSR-Izv.*, 82(3):522–540, 670–671, 1989.

[42] E. Landau. *Vorlesungen über Zahlentheorie I.* S. Hirzel, 1927.

[43] S. Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 1978.

[44] S. Lang. *Number theory III: Diophantine geometry*. Encyclopaedia of Mathematical Sciences. Springer-Verlag, 1991.

[45] Ju. I. Manin. Cyclotomic fields and modular curves. *Uspehi Mat. Nauk*, 26(6(162)):7–71, 1971.

[46] Ju. I. Manin. Parabolic points and zeta-functions of modular curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:19–66, 1972.

[47] D. Masser and J. D. Vaaler. Counting algebraic numbers with large height II. *Trans. Amer. Math. Soc.*, 359(1):427–445, 2007.

[48] G. Maze, J. Rosenthal, and U. Wagner. Natural density of rectangular unimodular integer matrices. *Linear Algebra and its Applications*, 434(5):1319–1324, 2011.

[49] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math*, 44(2):129–162, 1978.

[50] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[51] F. Mertens. Ueber einige asymptotische Gesetze der Zahlentheorie. *J. Reine Angew. Math.*, 77:289–338, 1874.

[52] J. S. Milne. On the arithmetic of abelian varieties. *Invent. Math.*, 17:177–190, 1972.

[53] T. Miyake. *Modular forms*. Springer Monographs in Mathematics. Springer, 1989.

[54] D. Mumford. *Abelian Varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay, by Oxford University Press, 1970.

[55] M. R. Murty and V. K. Murty. Mean values of derivatives of modular L-series. *Ann. of Math. (2)*, 133(3):447–475, 1991.

[56] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*. Springer, 2000.

[57] J. E Nymann. On the probability that k positive integers are relatively prime. *J. Number Theory*, 4(5):469–473, 1972.

[58] E. E. Pyle. Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components over $\overline{\mathbb{Q}}$. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 189–239. Birkhäuser, Basel, 2004.

[59] J. Quer. $\mathbb{Q}$-curves and abelian varieties of GL_2-type. *Proc. London Math. Soc.*, 81:285–317, 2000.

[60] K. A. Ribet. Galois representations attached to eigenforms with Nebentypus. *Lecture Notes in Math.*, 601:17–51, 1977.

[61] K. A. Ribet. Twists of modular forms and endomorphisms of abelian varieties. *Math. Ann.*, 253:43–62, 1980.

[62] K. A. Ribet. Abelian varieties over $\mathbb{Q}$ and modular forms. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 241–261. Birkhäuser, Basel, 2004.

[63] D. Rohrlich. Modular curves, Hecke correspondences and L-functions. In G. Cornell, J. Silverman, and G. Stevens, editors, *Modular forms and Fermat's last theorem*, pages 41–100. Springer-Verlag, 1997.

[64] S. Schanuel. Heights in number fields. *Bull. Soc. Math. France*, 107(4):433–449, 1979.

[65] J.-P. Serre. *Corps locaux*. Publications de l'institut de mathématique de l'université de Nancago. Hermann, 1968.

[66] J.-P. Serre. Modular forms of weight one and Galois representations. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 193–268. Academic Press, London, 1977.

[67] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math.*, 88(3):492–517, 1968.

[68] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publ. Math. Soc. Japan*. Iwanami Shoten and Princeton University Press, 1971.

[69] G. Shimura. On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields. *Nagoya Math. J.*, 43(171):199–208, 1971.

[70] G. Shimura. Class fields over real quadratic fields and Hecke operators. *Ann. of Math. (2)*, 95:130–190, 1972.

[71] J. H. Silverman. *The Arithmetic of Elliptic Curves*. GTM. Springer, 2009.

[72] D. Simon. Computing the rank of elliptic curves over number fields. *LMS J. Comput. Math.*, 5:7–17 (electronic), 2002.

[73] B. D. Sittinger. The probability that random algebraic integers are relatively r-prime. *J. Number Theory*, 130(1):164–171, 2010.

[74] C. Skinner. A converse to a theorem of Gross, Zagier, and Kolyvagin. `http://arxiv.org/abs/1405.7294`, 2014.

[75] W. A. Stein et al. *Sage Mathematics Software (Version 6.5)*. The Sage Development Team, 2015. `http://www.sagemath.org`.

[76] G. Stevens. *Arithmetic on modular curves*, volume 20 of *Progress in Mathematics*. Birkhäuser, 1982.

[77] J. Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 306, 415–440. Soc. Math. France, Paris, 1995.

[78] C. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.

[79] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math.*, 141(3):443–551, 1995.

[80] A. Wiles and R. Taylor. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math.*, 141(3):553–572, 1995.